
DEFENDING THE BORDERLAND

Ukrainian Military Experiences with IO, Cyber, and EW

By Aaron F. Brantly, Nerea M. Cal and Devlin P. Winkelstein



2017



**ARMY CYBER
INSTITUTE**
AT WEST POINT



ARMY CYBER INSTITUTE

AT WEST POINT

The Army Cyber Institute at West Point is a national resource for research, advice and education in the cyber domain, engaging military, government, academic, and industrial cyber communities in impactful partnerships to build intellectual capital and expand the knowledge base for the purpose of enabling effective Army cyber defense and cyber operations.

The views expressed are those of the contributing authors and do not reflect the official position of the United States Military Academy, Department of the Army or the Department of Defense.

About the Authors

Dr. Aaron F. Brantly is Assistant Professor in the Department of Political Science at Virginia Polytechnic and State University, Affiliated Faculty at the Hume Center for National Security and Technology, Cyber Policy Fellow at the Army Cyber Institute and Cyber Fellow at the Combating Terrorism Center. He holds a Ph.D. in Political Science from the University of Georgia and a Master's of Public Policy from American University. His research focuses on national security policy issues in cyberspace including big data, terrorism, intelligence, decision-making and human rights. His most recent book is the "Decision to Attack: Military and Intelligence Cyber Decision-Making" published by the University of Georgia Press.

MAJ Nerea M. Cal is an active duty Army officer serving as an International Relations instructor in the Department of Social Sciences and a Resident Fellow at the Modern War Institute at the United States Military Academy. She commissioned in 2006 from West Point and has served in the Army for eleven years as a Blackhawk pilot, including assignments to Iraq, Afghanistan, South Korea, and as an Air Assault Blackhawk Company Commander in the 82nd Airborne Division. Nerea earned a Masters in Global Affairs from Yale's Jackson Institute for Global Affairs and has published work relating to post-conflict reconstruction in Kosovo and the application of international law in cyberspace.

MAJ Devlin P. Winkelstein is an active duty Army officer and an International Relations instructor at the United States Military Academy. He commissioned as an infantry officer in 2006 from West Point and has served in a variety of assignments, including deployments to Iraq and Afghanistan. Devlin's most recent operational position was as a Stryker Company Commander in the 2nd Infantry Division. He earned a Masters of Arts in Government from Georgetown University and a PhD from Georgetown's Department of Government. His research focuses on civil conflict and the economics of international security agreements.

Acknowledgements: We wish to express our gratitude to Dr. Corvin Connolly, MSG Jeffery Morris, the Ukrainian Embassy in the United States, the personnel in the United States Embassy in Ukraine, the Asymmetric Warfare Group, the Cyber Conflict Studies Association, and all of our Ukrainian counterparts.

Table of Contents

I. Introduction.....	3
Ukraine in Context	3
Contextualizing the Current Crisis.....	4
What is Hybrid War?	5
Research Question.....	9
Methodology	10
Major Takeaways	10
II. Vulnerabilities.....	13
Military Force on Force Vulnerabilities	14
Political-Economic Vulnerabilities.....	17
Exploiting Vulnerabilities.....	21
Part III. Military Challenges in Ukraine	22
Cyber, EW, and IO in Ukraine at the Tactical Level.....	24
Tactical Cyber	25
Tactical EW	31
Tactical Information Operations	35
Tactical Cyber, EW and IO Advances and outcomes.....	39
Cyber, EW, and IO at the Operational Level in Ukraine.....	40
Training	40
Development and Acquisition of Resources	45
The Operational Impact.....	47
The Strategic Level of Cyber, EW, and IO in Ukraine.....	49
IV. Recommendations.....	55

***I**ntroduction*

Ukraine in Context

Ukraine is currently experiencing a conflict in two separate regions within its boundaries that challenges traditional conceptions of war, intervention, international law, and peacekeeping. The involvement of foreign military forces, unaffiliated foreign fighters, domestic rebels, irregular military units, and civilians in the conflict it a case study in hybrid warfare. This report seeks to understand the current state of hybrid warfare in Ukraine with a particular emphasis on the use of Information Operations (IO), Electronic Warfare (EW), and Cyber Operations (CO). We examine Ukraine's technical, training, political-legal, financial, and cultural vulnerabilities and illustrate how Russian and Russian-backed actors have tailored their IO, CO, and EW operations in Ukraine to exploit these vulnerabilities to achieve their strategic objectives. This model of hybrid warfare has affected Ukraine militarily and domestically and has had geopolitical implications within the region and the broader international community. We argue that the conflict in Ukraine serves as a testing ground for a new, more complex and dynamic form of hybrid warfare for which the United States Army and Department of Defense (DoD) must be prepared. Developing a robust and detailed understanding of the conditions that enabled this style of warfare and how Russia has exploited those conditions in Ukraine will serve to inform strategists and decision-makers of the measures that must be taken to prevent or counter future uses.



The context in which hybrid warfare has transpired in Ukraine is important as it forms the starting point for all subsequent findings on the impact of cyber, IO and EW on Ukraine's military and society. This report focuses on the military impact of hybrid warfare, a future report building on these findings will focus on the societal impact.

Our analysis is based on two weeks of in country meetings conducted with members of the Ukrainian government, military leadership and rank and file, volunteer battalions, members of the academic community, military industrial and commercial sectors as well as civilians. The result is an analytical work that provides an array of insights into many of the technical and societal aspects of a complex conflict.



Photo By Mstyslav Chernov

Contextualizing the Current Crisis

President Viktor Yanukovych's reversal of an earlier decision to sign an economic association agreement with the EU in November 2013 served as the catalyst for a series of events that has led to sustained hostilities in Eastern and Southern Ukraine. The association agreement would have continued the Westward trajectory and alignment of Ukraine with Western Europe. Yanukovych's failure to sign the agreement sparked mass protests and civil unrest known globally as Euromaidan and locally as the Revolution for Dignity. The protests lasted for 94 days and concluded when President Yanukovych fled the country to seek refuge in the Russian Federation on February 22, 2014. As the revolution unfolded, hundreds of thousands of Ukrainians from across the country flocked to the capital city of Kyiv and to their regional capitals to protest against the Yanukovych government. The protests were marred by significant violence that resulted in the deaths of more than 100 Ukrainian citizens.



Photo By blu-news.org (Ukraine Demo München)

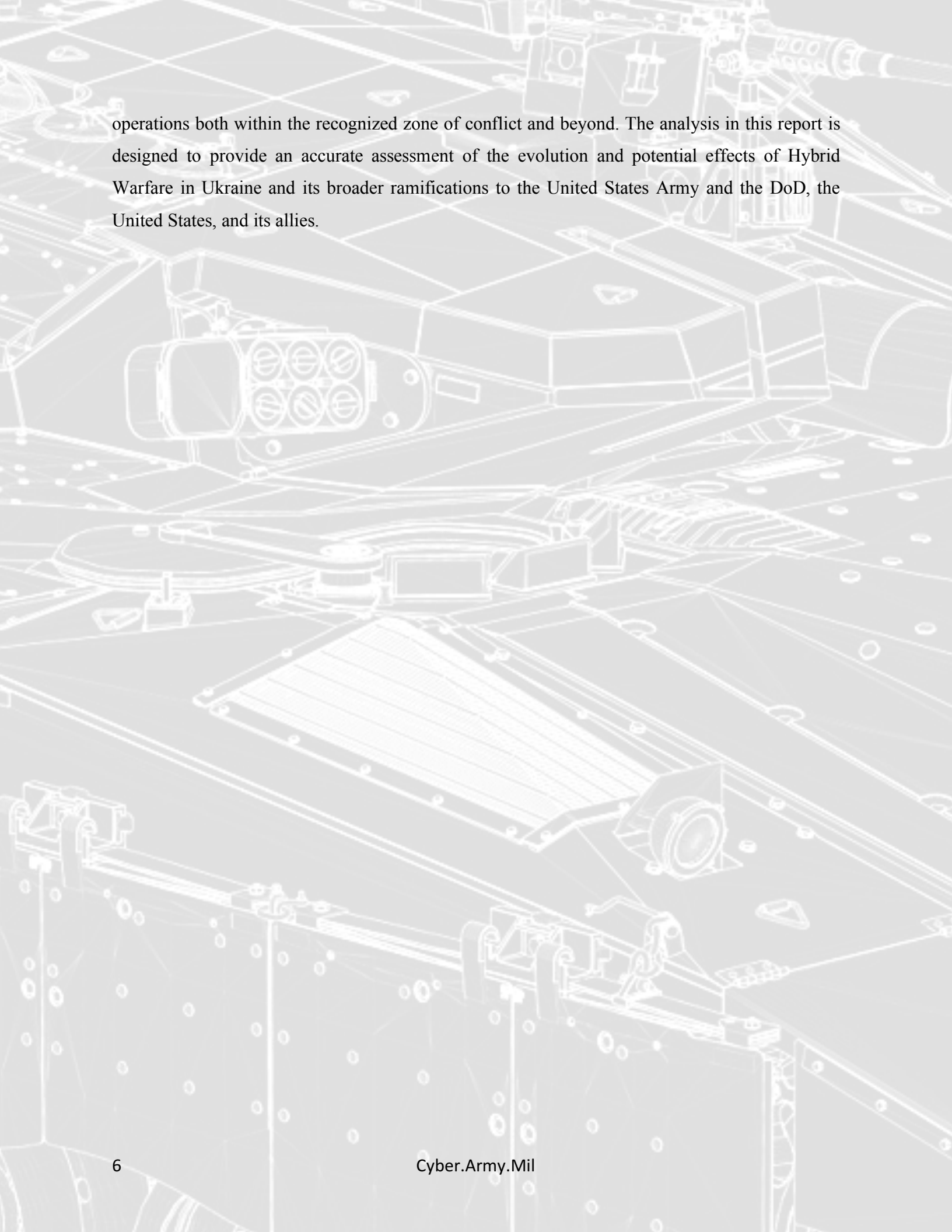
The aftermath of the political and social upheaval in Ukraine has had substantial economic, political, military, and territorial effects. Days before the collapse of the Yanukovych government, Russia inspired and mobilized protests in Crimea. Within 22 days of Yanukovych's departure the Russian Federation had successfully secured physical control over the entire Crimean Peninsula and held a referendum on annexation. Similar Russian-backed protests against the nascent Ukrainian government broke out in Eastern Ukraine, and between July and August 2014,

the Russian Federation deployed soldiers and military supplies to Ukraine under the guise of a “humanitarian convoy” in coordination with segments of the Russian speaking populations of Donetsk and Lugansk Oblasts. At the time of Russia’s mobilization, Ukraine had an active military force of 129,950 soldiers. Of these, only 6,000--or one to two brigade--were combat-ready. These units, along with the police and border forces in the Donbas, were quickly overwhelmed by the unrest and the scale of the evolving conflict. In the absence of a coordinated national military response, 40 to 50 Ukrainian volunteer battalions of varying size and skill levels rushed to the Donbas from dozens of geographic regions across the country. These battalions halted the advance of Russian forces, and a stalemate evolved that continues to the time of this writing.

Between March 2014 and June 2017, the Ukrainian military has undergone increasing professionalization and standardization. The volunteer battalions in the Donbas have been absorbed or replaced by active Ukrainian military units. Nevertheless, the conflict within the southeastern portions of Ukraine remains active and contentious. The zone of conflict extends hundreds of kilometers within the interior jurisdiction of Ukraine and has seen some of the most violent fighting on the European continent since the Balkan wars of the 1990s, resulting in more than 10,000 casualties.

What distinguishes the Ukrainian conflict from other modern conflicts is the manner in which the fighting has unfolded. More than any other conflict, the fighting in Ukraine has incorporated a wide array of methods: conventional tactics, CO, EW, and IO are employed in an overlapping and mutually reinforcing manner. Moreover, the conflict as a whole has been deliberately maintained at a level insufficient to warrant substantial outside intervention by the Europeans or Americans beyond limited programs to train and equip Ukrainian military and civilian security forces. Thus, the current conflict in Ukraine falls within a “gray zone” between all-out war and sustained hostilities. Moreover, although the Ukrainian actors within the conflict are quite clear, the actors fighting against Ukrainian forces are a mix of local rebels, foreign fighters, and Russian Federation regular and special forces.

The combined challenges of low-levels of sustained conflict, unclear combatants, and the diverse application of physical, informational, electronic, and cyber force against both recognized Ukrainian combatants along the line of demarcation and Ukrainian citizens throughout the country represent a novel use of power to achieve political objectives. It is the intent of this report to delve into the details of this ongoing conflict, with particular emphasis placed on EW, cyber and IO



operations both within the recognized zone of conflict and beyond. The analysis in this report is designed to provide an accurate assessment of the evolution and potential effects of Hybrid Warfare in Ukraine and its broader ramifications to the United States Army and the DoD, the United States, and its allies.



What is Hybrid War?

War has always been a complex construct that combines both physical, psychological and economic tools for the attainment of political ends. Examining the conflicts in which the United States has been engaged since World War II highlights the reality that formal declarations of war have largely fallen out of favor. Yet, at the same time there are clear instances where conflicts between states exceed the threshold of interventions, peacekeeping or other lower levels. International law attempts to define the characteristics of war and peace through various briefs and resolutions, the most robust of which is General Assembly resolution 3314 outlining “Crimes against Peace.” Despite these and other attempts to codify a type of conflict, it can often be challenging to distinguish between what is and is not war. The absence of the application of law and the creation of legal and jurisdictional gray zones exposes states, in particular weaker states, to exploitation by more powerful rivals. It is within this gray zone that states are able to leverage a series of levers of power forming a “hybrid” means of warfare.

To analyze the conflict in Ukraine we are deliberately focusing on it in the context of a gray zone conflict that leverages hybrid forms of warfare to achieve political, strategic, operational and tactical effects. The use of the term hybrid is not meant to be controversial and instead serves as a framework within which to analyze the levers of power being utilized by the opposing forces. As with any research endeavor it is important clearly define what we are analyzing. Below we are specifically interested on the utilization and impact of IO, EW, and CO within the confines of a constrained conflict situation or Hybrid war. In doing so, we build on two definitions of hybrid conflict. The first definition established by Frank Hoffman defines hybrid threats as:

Hybrid threats incorporate a full range of different modes of warfare including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder.¹

Hoffman's definition of hybrid conflict was further deepened in the *2015 Military Balance* produced by the International Institute of Strategic Studies and redefined as:

Sophisticated campaigns that combine low-level conventional and special operations; offensive cyber and space actions; and psychological operations that use social and traditional media to influence popular perception and international opinion.²

Combined, these two definitions frame the space in which we analyze the current conflict in Ukraine. We recognize the limitations of these definitions, but find that they are the most applicable methods for framing for the Ukrainian situation.

The current conflict in Ukraine falls within a “gray zone” between all-out war and sustained hostilities. Moreover, although the Ukrainian actors within the conflict are clearly identifiable, the actors fighting against Ukrainian forces are a mix of local rebels, foreign fighters, and Russian Federation regular and special forces. The combined challenges of low-levels of sustained conflict,

¹ Hoffman, Frank G. 2007. *Conflict in the 21st Century: the Rise of Hybrid Wars*. Arlington, VA: Potomac Institute for Policy Studies. P8.

² 2015. “Chapter One: Directed Energy Weapons: Finally Coming of Age?” *The Military Balance* 115: IISS. (1): P17.

unclear combatants and diverse applications of physical, informational, electronic, and cyber force against both recognized Ukrainian combatants along the line of demarcation and against Ukraine and its citizens have generated a novel use of power to achieve political objectives. It is the intent of this report to delve into the details of multiple aspects of this ongoing conflict, with particular emphasis placed on EW, cyber and IO operations both within the recognized zone of conflict and beyond. The analysis in this report is designed to provide an accurate assessment of the evolution and potential effects of hybrid conflict in Ukraine and its broader ramifications to the US Army, the DoD, the Nation, and allies.

Research Question

Our analysis is based on two weeks of in country meetings conducted with members of the Ukrainian government, military leadership and rank and file, volunteer battalions, members of the academic community, military industrial and commercial sectors as well as civilians. The result is an analytical work that provides an array of insights into both the technical and societal aspects of a complex conflict.

Our research team spent two weeks in Ukraine investigating the cyber, EW, and IO elements of the ongoing conflict Ukraine-Russia. The team's mandate from the Army Cyber Institute (ACI) was to write an unclassified report to help the U.S. Army and the DoD anticipate and prepare for future cyber, EW, and IO threats. During our trip, we met with government officials, academics, business leaders, journalists, soldiers, and private citizens to gather a diversity of perspectives on the current situation in Ukraine. Ukraine presented an ideal opportunity to observe firsthand the latest developments in cyber, EW, and IO within the broader context of hybrid warfare, which we define in accordance with Hoffman and the IISS as the flexible combination of conventional, unconventional, political, and economic means to achieve strategic ends while avoiding a broader international conflict. It is increasingly clear that hybrid warfare will be an important form of modern warfare in the 21st Century, and this reports adds to a growing body of literature on the topic.³ We hope this report will contribute to this literature and help

³ 2016. "Hybrid Warfare: a New Phenomenon in Europe's Security Environment." Prague: NATO Information Centre; Renz, Bettina, and Hanna Smith. 2016. "Russia and Hybrid Warfare: Going Beyond the Label." Aleksanteri Institute; Radin, Andrew. 2017. "Hybrid Warfare in the Baltics: Threats and Potential Responses." RAND Corporation.

inform decision makers as they structure and equip U.S. security forces when addressing current threats.


Methodology

The crisis in Ukraine spans multiple dimensions, each of which requires attention. However, our focus falls within the mandate of the ACI and focuses on the interplay of cyber, EW, and IO in a sustained “gray zone” of conflict often referred to as hybrid warfare. This report is organized around Ukraine’s vulnerabilities to threats originating from non-Ukrainian and Ukrainian actors and the environment in which the country finds itself. Many of the threats have been directly linked or have strong supporting evidence of Russian Federation involvement. Within the context of a hybrid conflict in Ukraine, threat and vulnerability go hand-in-hand. The mix of tools employed in Ukraine combine to uniquely exploit the vulnerabilities created by Ukraine’s particular geographic, economic, demographic, political, and historical characteristics. Many of the threats have been directly linked or have strong supporting evidence of Russian Federation involvement and align closely with current Russian doctrine and geostrategic objectives.⁴

This report relies information attained during meetings held between June 21st and July 1st in Kyiv and Lviv with members of Ukraine’s corporate, academic, civil society, government, and national security sectors. Additional primary and secondary sources are used for contextualization of the information garnered through the various meetings. The intent is to provide an unbiased and unvarnished look at the current status of Ukraine’s military readiness to address an evolving threat environment.

From June 21 through July 1 a team of four members of the United States Army Cyber Institute and US Army Cyber Center of Excellence engaged in meetings with Ukrainians from multiple sectors. The members of the team were chosen for their backgrounds in cyber security training, policy, law and international relations. Meetings were held in Kyiv and Lviv Oblasts within Ukraine, and each meeting attempted to address issues related to the present status of organization within military and civilian governmental structures in relation to cyber, EW, and IO.

⁴ Giles, Keir. 2016. “Handbook of Russian Information Warfare.” NATO Defense College; Isabelle, Facon. 2017. “Russia’s National Security Strategy and Military Doctrine and Their Implications for the EU.” Policy Department, DG EXPO - European Parliament; Путин, Владимир. 2010. “Военная Доктрина Российской Федерации.” *Президент России*. February 5. <http://kremlin.ru/supplement/461>.

The background of the page is a detailed, light gray technical drawing or wireframe of a mechanical assembly, possibly a vehicle chassis or a complex machine. It features various components like beams, joints, and a circular element that looks like a wheel or a large bearing. The drawing is composed of numerous thin lines and dots, giving it a schematic or blueprint appearance.

The meetings followed a semi-structured interview format with a detailed list of questions covering all aspects of cyber, IO and EW prepared in advance of the trip. This question list served as a starting point for discussions with Ukrainian counterparts and was tailored to account for matters of particular relevance and political sensitivities within various meetings. Our questions emphasized the organization and capacity of various government and national security actors to address threats both within the zones of conflict and across the nation. For meetings with non-governmental entities including academic institutions, military industrial firms, cybersecurity firms and former soldiers within Ukrainian volunteer battalions the intent was to assess perceptions of government capacity and organization, societal strength and resilience. This report deliberately does not provide individuals' names. Instead, we refer to higher level organizational structures or sectors. The intent is to provide as much relevant context as possible while safeguarding those with whom we met against potential negative consequences related to our discussions.

We organize the remainder of this report as follows. In Part II, we describe Ukraine's particular mix of military and political-economic vulnerabilities to cyber, EW, and IO attacks. In Part III, we analyze the ways in which the Russian Federation and Russian-backed actors have exploited Ukraine's vulnerabilities and the effects of that exploitation at the tactical, operational, and strategic levels of the ongoing conflict. Finally, in Part IV, we make recommendations how the United States should approach the situation in Ukraine. As noted above, this report focuses on the military dynamics and implications of hybrid warfare in Ukraine, and a future report will take-up the political and economic implications.

Major Takeaways

- Ukraine is largely reactive to threats emanating both internally and externally to its jurisdictional boundaries in cyberspace, information operations and electronic warfare.
- The reactive nature of Ukraine's response to cyber, EW, and IO threats is due to constrained human and financial capital within the government, military and national security sectors. These constraints include low pay and poor opportunities for career growth for skilled personnel as well as widespread shortcomings in equipment and resources available to combat a wide array of threats.
- Ukraine has taken enormous strides within its security services and national police to include the development of organizational structures and the allocation of significant resources to combat cyber, EW, and IO threats. The least amount of development has occurred within the military, where organizational structures have been established but a severe lack of both human and financial capital has hampered an effective response to battlefield threats.
- Due to political issues both within the Verkhovna Rada and the bureaucracy of Ukraine, the sub-agencies under the NSDC have widely divergent capacities, roles and responsibilities. There is evident tension between the military and security services with the State Service for Special Communication attempting to act as a political mediator between them and other constituent agencies within the NSDC on issues related to cybersecurity and defense. It is clear that the majority of state capacity resides within the security services or in the defense industrial base/private sector.
- Ukraine has a robust educational and training capacity within its universities, but there is a lack of funding for equipment, training, and resources. Although faculty and students are increasingly interested in addressing the pressing challenges faced by Ukraine, physical resources for programs across the report's focus areas within this report are substantially lacking. This lack of resources constrains the pipeline for human capital needed to engage a complex threat environment.
- The combined threat environment of stemming from the use of cyber, EW, and IO across the conventional, economic, and political sectors of conflict merge to create a societal siege mentality under which Ukrainian citizens and their government must operate on a daily basis.



Vulnerabilities

For the purposes of this report, vulnerability is defined as exposure to the possibility of being attacked or harmed, either physically or emotionally.” In this case, we are particularly interested in vulnerabilities that expose Ukraine to the class of tactics and tools encompassed by cyber, EW, and IO. We examine each vulnerability to ascertain: what the vulnerability is; where it comes from and why; how the vulnerability specifically affects Ukraine; how Russia and Russia-aligned actors sought to exploit the vulnerability; and, lastly, how the vulnerability fits within a hybrid warfare framework.

We divide Ukraine’s vulnerabilities into two categories: military (force on force) and political-economic. This division was chosen for the following reasons: First, conflict between organized military forces occurs within a different legal-normative framework than internal or international issues such as propaganda in the media, hacking of government systems, and infrastructure attacks. The associated legal-normative issues constitute one of the central challenges of hybrid warfare: how should a country respond without triggering a declared war when an adversary simultaneously militarily and societally threatens the security of a state? Second, the conceptual distinction between military and political-economic vulnerabilities highlights the ways that the Russian Federation exploits both military and political-economic targets in Ukraine using cyber, EW, and IO within a synchronized campaign. By considering Ukraine’s military and political-economic vulnerabilities separately and as interactive parts of a single campaign, we are able to examine the complexity of the cyber, EW, and IO components of the conflict in detail and how they degrade Ukraine’s capacity to maintain its national security and provide services for its citizenry.

Military Force on Force Vulnerabilities

Ukraine's military vulnerabilities stem in large part from its disadvantages relative to the Russian military apparatus. At the end of the Cold War in 1992, Ukraine boasted one of the largest standing militaries in the world and the third largest nuclear arsenal. Its military consisted of 430,000 active duty troops.⁵ More than 25 years later, a combination of neglect and misguided policy decisions have left Ukraine's military unable to field significant offensive or defensive forces. In March 2014 Ukraine had an active duty military force of 140,000 with only two combat ready brigades totaling 6,000 poorly supplied personnel using antiquated equipment. Additionally, endemic corruption within the Ministry of Defense created a weakened command and control structure.⁶

In contrast, the Russian Federation had adapted lessons learned from the 2008 Russia-Georgia War and continued conflicts in Chechnya and Syria to develop a robust training and logistical structure within its Southern Military District, which stretches from Georgia in the Southeast to the Ukrainian border along the West. Although military corruption remains a significant problem in the Russian military, these improvements in the Southern Military District, reconfigurations of command and control, and a complete overhaul of special forces capabilities have significantly strengthened Russia's offensive capabilities in recent years.⁷

At the start of hostilities between Ukraine and the Russian Federation in March 2014, the balance of forces between the two nations was heavily skewed in Moscow's favor. First and foremost, Ukraine had, at the beginning of hostilities, an organizational problem. Despite periodic joint exercises with NATO partners the Ukrainian military was primarily structured, managed and operated as it was at the collapse of the Soviet Union in 1992. Vyacheslav Tseluyko writes the Ukrainian military forces were largely in a state of "suspended animation."⁸ Moreover, numerous sources cited endemic corruption both within Ukrainian government and more specifically the

⁵ World Bank. Data from the International Institute for Strategic Studies, the Military Balance. Accessed 7 Nov 2017. <https://data.worldbank.org/indicator/MS.MIL.TOTL.P1?locations=UA>

⁶ Howard, Colby, and Ruslan Pukhov. 2015. *Brothers armed: military aspects of the crisis in Ukraine*. Minneapolis: East View Press.

⁷ Bukkvoll, Tor. 2016. "Russian Special Operations Forces in Crimea and Donbas." *Parameters* 46 (2): 1–10.

⁸ Tselyyko, Vyacheslav. "Rebuilding and Refocusing the Force: Reform and Modernization of the Ukrainian Armed Forces." in Howard, Colby, and Ruslan Pukhov. 2015. *Brothers armed: military aspects of the crisis in Ukraine*. Minneapolis: East View Press.

Ukrainian military over the duration its independence until 2014.⁹ Out of 82 countries Ukraine's military corruption ranks in the middle third with a corruption ranking of D+ on a A to F scale.¹⁰ Although by no means the most corrupt, Ukraine's inefficiencies in managing every aspect of its military placed it in a severely weakened state. Moreover, military expenditures were relatively low in comparison to other programs.

Military force on force vulnerabilities within Ukraine at the start of hostilities in 2014 was a recurrent point of discussion during every meeting held during our trip. High-level government officials within the Ministries of Defense, Foreign Affairs, Security Services, as well as representatives from the defense industrial base, academia, civilian technology companies, citizens and soldiers returned from the field universally noted organizational, resource and leadership deficiencies that made the provision and management of a sustained response to Russian and domestic rebel forces extremely difficult. Most meetings noted that after the collapse of the Yanukovych regime the systemic penetration of the intelligence services, military and other organizations, endemic neglect and corruption placed Ukraine in a severely weakened state. One particularly prescient story told was that of the state of the offices of the SBU (Ukraine's Security Service). As told to us by a source with firsthand knowledge, in the immediate aftermath of the regime's collapse the SBU executive offices were ransacked and files stolen or destroyed. The incoming SBU leadership was tasked with reconstituting the security services under the threat of persistent and sustained penetrations. Similar problems were faced by the Ministry of Defense.

In the initial phases of hostilities, Ukraine could muster only 6,000 soldiers to send to the front lines, and the inadequate state of force readiness created multiple cascading force-on-force vulnerabilities. First, Ukrainian command structures, particularly in Crimea failed to provide adequate direction to forces. Second, human resources proved insufficient to quickly and effectively confront an escalating security situation along a large territorial boundary with the Russian Federation and internally within Ukraine. Third, physical resources within the armed forces were inadequate to counter more advanced Russian equipment, manage the provision of rations to soldiers and provide medical support to casualties. In response to these shortcomings, Ukrainian citizens stood up multiple volunteer battalions that were privately trained and provisioned both organically (with citizen support) and with the support of specific oligarchs.

⁹ 2006. "Corruption Assessment: Ukraine." United States Agency for International Development; Osipian, Ararat L. 2010. "Corrupt Organizational Hierarchies in the Former Soviet Bloc." *Transition Studies Review* 17 (4): 822–36; 2013.

¹⁰ "Government Defence Anti-Corruption Index 2013." Transparency International UK.

While essential to stopping Russia's advance, these volunteer battalions introduced additional vulnerabilities, especially in the areas of communications and command and control.

More than three years later many of the initial problems associated with force-on-force vulnerabilities have been addressed in part or whole. All forces currently serving along the contact line in Ukraine are currently under the control of the Ministry of Defense, or the State Border Guard Service of Ukraine. With assistance from European and US partners the Ukrainian military, police and border units have engaged in substantial training and capacity development. The operational readiness of Ukraine's military, police and border units has changed substantially for the better. Although there are some definite gaps that still exist, the perceptions within meetings with government officials and among both soldiers and civilians is that substantive improvements have been made.

Among the gaps that remain is the provisioning of soldiers, police and border units with modern equipment that allows them to achieve technical parity with Russian adversaries. Secure communications remain an area of significant concern for both commanders and soldiers. Communications issues will be addressed more explicitly in later sections. Ukrainian government officials focused their comments and requests for support on the availability of equipment and training that would allow them to achieve defensive parity for territorial defense against the Russian Federation. Across in meetings there was no mention of engaging in offensive military operations leveraging either kinetic or digital/electromagnetic means. The consistency of responses on the subject of training and equipment highlights a perception that Western equipment is superior to or at the very least allows Ukrainian forces to maintain defensive positions. Several times over the duration of our visit various groups expressed gratitude for the delivery of AN/TPQ-36 radar systems (Counter Battery Radar Systems) and expressed hopes for additional resources.

Medical services and provisions to Ukrainian soldiers are perceived to have improved, but have not reached adequate levels according to soldiers. The increasing professionalization of Ukraine's armed forces is evident. Soldiers are being actively recruited from civilian populations using a variety of print, radio, TV, and digital media. Recruitment is hampered by casualty rates on the Ukrainian side of the conflict that remain relatively consistent. The psychological impact of the ongoing fighting remains visible across the nation. One day before to our visit to Boryslav in Lviv Oblast, the entire population of the town turned out to bury two soldiers killed in the ATO. The day of our departure from Kyiv to Boryslav, a targeted bombing resulted in the successful

assassination of Lieutenant Colonel Oleksandr Kharaberiush, deputy chief of the Donetsk region counterintelligence department for the Ukrainian Security Service (SBU). Also, on the day of our departure from Kyiv to Lviv massive cyber-attacks crippled large swaths of Ukraine's infrastructure.

The ability to solve military force-on-force vulnerabilities does not occur in a vacuum and Ukraine has been forced to manage multiple reform and modernization challenges in the midst of a both defined conflict zones and across the country as a whole. These organizational and modernization efforts have been severely constrained by Ukraine's economic depression that has seen the value of its currency, the Hryvnia, plummet making the procurement of foreign goods, in particular military hardware, within a limited fiscal reality nearly impossible and challenges modernization, training, and provisioning efforts.

Financially, Ukraine's armed forces, border guards, police and security services are overmatched. The imbalance between the funding of Russian forces and the consistent stream of men and material and those of Ukrainian forces are likely to remain in the years to come. The more established, organized and financed defense industrial base, leadership structures, and training pipelines within the Russian Federation are unlikely to be matched by Ukrainian forces. Although Ukrainian forces might achieve measures of parity within specific areas, persistent long-term and irreconcilable vulnerabilities in cyber, EW, and IO should inform strategy, operations and tactics.

Political-Economic Vulnerabilities

The fall of the Soviet Union left most former Soviet republics in a state of governmental and economic disarray. The transboundary economic structures developed under the Soviet Union resulted in substantial economic difficulties when the internal boundaries became transnational. Moreover, the political leadership the early post-Soviet years was derived from former Communist party leadership. Ukraine's first President was the former Chairman of the Supreme Soviet of the Ukrainian Soviet Socialist Republic. In addition to the complex political ties between Russia and Ukraine, the histories, economies, languages, industries and societies of Ukraine and Russia are intertwined in a complex framework dating back hundreds of years. The establishment of a unique Ukrainian state, with a national identity, robust and independent economy distinct from that of the Russian Federation and the Soviet Union before it has been a matter of contention both within Ukraine and in the Russian Federation.

Political and economic vulnerabilities within Ukraine are numerous, yet a basic framing is necessary within this report because of a susceptibility of Ukraine to outside influence that impacts military readiness and capabilities at a societal level within a hybrid warfare context. Political and economic vulnerabilities are examined with respect to identity, historical relationship with Russia, the state of the economy, and geographic location within this subsection in four groupings. The examination of these groupings is of value within the military context because they provide potential vulnerabilities present at the level of the warfighter directly relevant to how soldiers fit within a Ukrainian nation.

First, the concept of political identity is and remains a contentious subject within Ukrainian domestic and international politics. Political identity within Ukraine is constructed through the linking of socio-cultural- and geographic attributes. construction since the Soviet legacy are defined and societal structures, religious practices. From Orthodox Christianity as

The inability to fall back on a consistent, single Ukrainian narrative or national language was identified as a point of weakness that exposed Ukraine to external manipulation.

religious, linguistic, historical Ukraine's formative years of Kievan Rus in 882 to its post-by overlapping ideas of social cultural attitudes and the establishment of the state religion under Vladimir the Great, linking Kyiv and Constantinople, to the establishment of the Kievan and Muscovite Patriarchies and the Polish influence through the introduction of Greek Catholicism (a hybrid between Orthodoxy and Roman Catholicism in which the Pope and not the Patriarch is the head of the Church) in Western Ukraine and finally the non-religious Soviet period, Ukrainian politics and religion have been intimately tied both internally to national identity and transnationally to broader notions of what constitutes the nation itself.¹¹ While religion itself forms one of the central constructs of Ukrainian society, Ukraine is also divided linguistically. Russian is the predominant language of urban eastern Ukraine, while Surzhyk (a Ukrainian/Russian mixture) is found in most rural eastern Ukrainian villages. The Ukrainian language is most common in Western portions of Ukraine, West of the Dnipro River. As one moves towards the center of the country the mix between Ukrainian and Russian becomes greater. The southern portions of Ukraine are mainly Russian speaking. Polling data on Ukrainians conducted by the

¹¹ Plokhyy, Serhii. 2015. *The Gates of Europe : a History of Ukraine*. New York: Basic Books; Wilson, Andrew. 2000. *The Ukrainians : Unexpected Nation*. New Haven: Yale University Press.

International Republican Institute in the years before the conflict indicate complex regional linguistic cleavages, these linguistic cleavages are closely mirrored by national and ethnic affinities towards either the Russian Federation and Soviet Union (East/South) and Ukrainian (West).¹²



Second, historically the concept of Ukraine is complex and involves a combination of historical facts and myths from both the Eastern and Western portions of the country.¹³ The appropriate mix of fact and myth has been analyzed by various scholars with each individual, region and oblast incorporating selective parts of a broader Ukrainian narrative. In discussions with faculty from Taras Shevchenko National University in Kyiv, the complexity of these divergent political identities was discussed and raised as a significant vulnerability. The inability to fall back on a consistent, single Ukrainian narrative or national language was identified as a point of weakness that exposed Ukraine to external manipulation. Beyond the measured academic assessment, we also heard from Ukrainians who upon walking with us in Kyiv's Pechersks Lavra (a large Russian Orthodox Church Complex) cautioned us against the voluminous amounts of disinformation coming from the Russian Orthodox Patriarchy to foster discord within Ukraine. Specifically, our local guide indicated funding, support and Russian influence emanating from the clergy with the intent of shaping the historical and psychological narrative of the country.

Third, Ukraine's economic landscape was racked by a mix of post-Soviet decay, corruption, foreign meddling and developmental malaise. In the immediate fall of the Soviet Union hyperinflation and burdensome state budgets created substantial economic hardships. With the introduction of a unified and independent currency, the Hryvnia, under the then Central Bank Chairman Viktor Yushchenko, the economy of Ukraine stabilized somewhat, but not without first seeing the transfer of large volumes of holdings away from workers to a newly formed class of

¹² International Republican Institute. 2013. "Public Opinion Survey Residents of Ukraine August 27-September 9, 2013." http://www.iri.org/sites/default/files/IRI_Ukraine_August-September_2013_Edited%20Poll.pdf.

¹³ Plokyh, Serhii. 2015. *The Gates of Europe : a History of Ukraine*. New York: Basic Books; Plokyh, Serhii. 2015. *The Gates of Europe : a History of Ukraine*. New York: Basic Books; Iinytzkyi, Oleh S. "'Imperial Culture' and Russian-Ukrainian Unity Myths" in Velychenko, Stephen. 2010. *Ukraine, the EU and Russia : History, Culture and International Relations*. Basingstoke: Palgrave Macmillan.

oligarchs who would come to dominate the economic and political landscape of Ukraine.¹⁴ The intimate relationship of oligarchic interests and national politics increased over the next 20 years and created a complex network of ties between the state and large business interests. While oligarchs achieved substantial wealth, the remainder of the population struggled with high interest rates and complex tax and regulatory codes making small and medium sized business ventures difficult to set up, manage, maintain and close.¹⁵

Further exacerbating and complicating relations between Ukraine and Russia are interwoven business interests within the oligarchies of Russia and Ukraine and legacies of post-soviet weapons manufacturing, largely centered in the eastern portions of Ukraine. The mesh of relationships and business networks led Russia to incentivize Ukraine to maintain it within its sphere of influence. Nowhere has Russian influence been stronger than in Ukraine's energy sector. Energy has been a consistent source of leverage and regional tensions between Ukraine and Russia.¹⁶ Russia provided discounted gas prices to induce politicians towards maintaining close ties. Gas has been used as a strategic weapon through the suspension of delivery to Ukraine and the suspension of transit across Ukraine in a manner of tit-for-tat politics.

Fourth, the geographic location of Ukraine has historically and continues to create international political problems for the nation. Ukraine's location in Eastern Europe bordering the Russian Federation and often considered to be intimately linked with historical concepts of Russian or Soviet spheres of influence, Ukraine struggles to build a truly Western identity that links it with potential allies in Western Europe and the US.¹⁷ Its proximity to Russia and the Russian Nuclear arsenal and potential threats posed by Russian military force to European Union member states along the Union's eastern frontier make achieving meaningful support difficult. Despite recent advances between the EU and Ukraine on visa restrictions and the development of an association agreement, the robustness of military and diplomatic assistance has been limited. Ukraine has instead received measureable support from post-Soviet states such as Poland within the EU.¹⁸ Although many of its European problems are domestically linked to corruption, energy dependence, rule of law and state capacity, the inability to develop a consistent and robust

¹⁴ Åslund, Anders. 2009. *How Ukraine Became a Market Economy and Democracy*. Washington, DC: Peterson Institute for International Economics.

¹⁵ Ibid.

¹⁶ Lee, Yusin. 2017. "Interdependence, Issue Importance, and the 2009 Russia-Ukraine Gas Conflict." *Energy Policy* 102 (C). Elsevier: 199–209.

¹⁷ Kuzio, Taras. 2016. "Ukraine Between a Constrained EU and Assertive Russia." *JCMS: Journal of Common Market Studies* 55 (1): 103–20.

¹⁸ Burlyuk, Olga. 2017. "Same End, Different Means: the Evolution of Poland's Support for Ukraine at the European Level." *East European Politics and Societies* 31 (2): 311–33.

relationship with the EU as a whole weakens Ukraine's position concerning Russia and within domestic populations.¹⁹

The religious, social-historical, economic and political vulnerabilities listed above are constitutive of only a few of the many areas ripe for Russian exploitation within Ukraine, however, they highlight four of the areas most exploited within the current conflict between Russia and Ukraine and are areas that will continue to be of significance in the years to come. The above areas outlined as vulnerable to hybrid forms of warfare result in a siege mentality within the broader population and weaken governmental management and organization of civilian and military functions of the state.²⁰


Exploiting Vulnerabilities

Military force on force and civilian political and economic vulnerabilities constitute two crucial yet distinct aspects of state security in the face of external threats. The remainder of this report focuses on the way in which the utilization of cyber warfare, EW, and IO exploit and exacerbate the vulnerabilities listed above within the military sector of Ukraine. The graphic at the beginning of this section illustrates the targeting of these vulnerabilities across strategic, operational and tactical levels within both civilian and military contexts. This report is the first of two reports on the impact of cyber, electromagnetic and information operations on Ukraine. This report emphasizes the military aspects of the conflict, while a planned future report will highlight civilian challenges.

Part II outlined the conditions that allow the tools discussed in the Part III to achieve effects. Below, we analyze force-on-force vulnerabilities at the tactical, operational, and strategic levels from a distinctly military perspective. The close examination of the tactical, operational and strategic levels is intended to provide perspective on the military aspects of a hybrid conflict. Organizing our analysis in this way allows for the development of recommendations and solutions at those levels of operation. While addressing many of the military challenges we must simultaneously examine some of the exploitation of political and economic vulnerabilities that extend beyond the military. By analyzing the impact of cyber, IO and EW attacks with respect to

¹⁹ Zafar, Shaista Shaheen. 2015. "The Ukraine Crisis and the EU." *Journal of European Studies*, December, 66.

²⁰ Brantly, Aaron F, Nerea Cal, Devlin Winkelstein. 2017. "Don't Ignore Ukraine: Lessons from the Borderland of the Internet." *Lawfare*. <https://www.lawfareblog.com/dont-ignore-ukraine-lessons-borderland-internet>



the development of policies and laws, we are better able to understand how these areas of Ukrainian society impact the military structures in Ukraine. Analyzing the military effects of cyber, EW, and IO reflects an appreciation for the complexities of hybrid warfare, which features the blending of traditional and unconventional tools to achieve wide-ranging effects.



Military Challenges in Ukraine

Cyber, EW, and IO are unique within the broader scope of hybrid warfare. There are many aspects of the conflict in Ukraine that have been analyzed across an array of reports, white papers, articles and blogs. Many of these prior works addressed broader aspects of the conflict within a geopolitical context or in the balance of power between two opposing forces. These reports are extremely valuable in contextualizing the nature of the conflict and its implications from the political or strategic level of analysis.²¹ Our objective in this report differs from these analyses by emphasizing what our Ukrainian counterparts identified as issues of importance to them with

²¹ Hunter, Eve, and Piret Pernik. 2015. "The Challenges of Hybrid Warfare." International Centre for Defense and Security; Daalder, Ivo, Michele Flournoy, John Herbst, Jan Lodal, Steven Pifer, James Stavridis, Strobe Talbott, and Charles Wald. 2015. "Preserving Ukraine's Independence, Resisting Russian Aggression: What the United States and NATO Must Do." Brookings; Renz, Bettina, and Hanna Smith. 2016. "Russia and Hybrid Warfare - Going Beyond the Label." Aleksanteri Institute; Rácz, András. 2015. "Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist." The Finnish Institute of International Affairs.

varying contexts associated with the prosecution of the conflict within Ukraine. While the report touches upon the political and strategic levels of analysis it does so in service of understanding the role that cyber, EW, and IO play within the hybrid warfare framework.

Part III explicitly focuses on what we identified through conversations with a wide range of actors associated with the Ukrainian military. We divide the analysis in this part across the tactical, operational and strategic levels from the perspective of the management of hybrid warfare within Ukraine from a military perspective. While we examine each level as discrete, we do so artificially and with full knowledge that they are continuously interacting and informing one another. We are also deliberately disaggregating the broader civilian structures party to the hybrid war in Ukraine from the military structures at the tactical, operational and strategic level to distinguish those aspects of the conflict more consistent with traditional conflict settings. Hybrid warfare spans the military and civilian line, yet the individuals engaged in addressing the ramifications of hybrid warfare in Ukraine largely do not span this divide. The one exception in the case of Ukraine is its security service which will be discussed below.

Cyber, EW, and IO in Ukraine at the Tactical Level

Distinctions between Cyber, EW, and IO are best found at the tactical level. Here the implementation of strategy and the success of operational activities result in either gains or losses. Gains and losses occur across territory, lives, intelligence, and equipment. Challenges in the tactical environment can lead to reductions in maneuverability and effectiveness of forces. While analyses on the tactical level of combat are common, very rarely in modern conflict has the usage of cyber, EW, and IO combined in a trifecta of complementary actions to alter the tactical situation between opposing forces. Although it is important to caveat that the use of EW and IO at the tactical level is not new, the manner in which they are being employed in the Ukrainian context and in combination with cyber operations is novel. Those areas where the impact of cyber, EW and IO were highlighted by our Ukrainian counterparts are discussed below.

Tactical Cyber

Cyber operations are constitutive of cyber-enabled offensive or defensive operations that occur over or across either physical, logical or Cyber-Persona layers of cyberspace.²² Tactical cyber operations occur close to or cross over the contact lines of opposing military or combatant forces with the intent of shaping maneuvers, engagements and battles. Tactics are “the employment and ordered arrangement of forces in relation to each other. Joint doctrine focuses this term on planning and executing battles, engagements, and activities at the tactical level to achieve military objectives assigned to tactical units or task forces.”²³

At the tactical level in Ukraine, the force on force weaknesses, in particular legacy hardware and equipment made the early stages of conflict largely immune to cyber-attacks against conventional weapon systems. Although structurally and organizationally at a disadvantage, the physical hardware did not suffer from cyber enabled exploitations. While the physical hardware of armored personnel carriers, tanks, field artillery and similar equipment was spared direct attacks emanating from cyberspace, the communications channels used to coordinate tactical movements suffered immensely. We found substantial evidence to confirm reports by Kyiv researcher Glib Pakharenko to indicate the targeting of mobile networks, Wi-Fi, mobile phones and other communications networks within military force structures both during the initial stages of conflict and continuing during current hostilities.²⁴ Targeted attacks against military communications and individual soldier (personal) communications were raised within the National Security and Defense Council, Members of the Ministry of Defense, former and current soldiers who fought in the Anti-Terrorism Operation (ATO) and foreign advisors who recently returned from the front lines.

Specific targets of cyber operations identified within discussions parallels that of earlier reports and included incidents of mobile phone intercepts using social media intelligence (SOCMINT), and the use of mobile cellular broadcast towers to intercept and manipulate the communications of soldiers and units operating within the area of hostilities.²⁵ Initial cyber exploits involved intelligence analysis of social media posts by Ukrainian soldiers. These posts alerted Russian and rebel forces to the presence and organization of Ukrainian soldiers allowing

²² 2013. *Joint Publication 3-12 (R), Cyberspace Operations*. Department of Defense. v.

²³ 2011. *JP 3-0, Joint Operations*. Department of Defense. xii.

²⁴ Pakharenko, Glib. “Cyber Operations at Maidan: A First-Hand Account” in Geers, Kenneth. 2015. *Cyber War in Perspective: Russian Aggression Against Ukraine*. Tallinn: NATO Cooperative Cyber Defense Centre of Excellence.

²⁵ Reynolds, Anna. 2016. “Social Media as a Tool of Hybrid Warfare.” Riga: NATO Strategic Communications Center of Excellence. 13.

for counter positioning. SOCMINT targeting, while not technically sophisticated, proved remarkably useful for both sides as well as international investigators in understanding the force structures and progress made on both sides of the contact line.²⁶ The social media environment within Ukraine greatly enhanced Russian visibility into Ukrainian social media habits as large percentages of Ukrainian citizens at the time of initial hostilities had at least one Russian social media service, most commonly VKontakte or Odnoklassniki.²⁷ The use of these social media services in tandem with other Russian online services such as the popular Mail.ru exposed soldiers who brought mobile devices to the front lines to exploitation. Through content analysis, image analysis and geotagging of metadata both sides were able to exploit the convenience of war fought within range of one's own cellular provider.

Although both sides took advantage of social media and mobile devices, Russia had numerous advantages including skilled signals intercept and analysis capabilities as well as direct access to the telecommunications firms providing mobile services to include Vodafone Ukraine a subsidiary of Мобильные ТелеСистемы (Mobile TeleSystems) of Russia. The landline communications systems of Ukraine were developed mainly during the Soviet era and include SORM (Система Оперативно-Розыскных Мероприятий or "System for Operative Investigative Activities"). SORM is a suite of technologies tracing their origins back to KGB research as Soviet telecommunications networks expanded. SORM-3 now "has the ability to target all forms of communication providing long-term storage of all information and data on subscribers, including actual recordings and locations."²⁸ Investigative journalists Andrei Soldatov and Irina Borogan highlight the immense capabilities of the SORM protocols to quickly and rapidly analyze virtually any form of digital communication.²⁹ In our discussions with Ukrainian officials, it was acknowledged that the implementation of these systems within Ukraine was likely susceptible to and had experienced Russian manipulation. The vulnerability of national telecommunications infrastructure to outside parties under the SORM protocol indicate that all non-encrypted communications over state telecommunications service providers would be vulnerable to intercept.

²⁶ Veli-Pekka. 2015. "Bellingcat Launches the Ukraine Conflict Vehicle Tracking Project - Bellingcat." *Bellingcat*. February 3. <https://www.bellingcat.com/resources/2015/02/03/ukraine-conflict-vehicle-tracking-launch/>.

²⁷ Borys, Christian. 2017. "Ukraine Bans Russian Social Media Sites in an Attempt to Punish the Kremlin." *Vice News*. Accessed October 3. <https://news.vice.com/story/ukraine-bans-russian-social-media-sites-in-an-attempt-to-punish-the-kremlin>.

²⁸ 2014. "The Russia-Ukraine Cyber Front Takes Shape." *Recorded Future*. March 7. <https://www.recordedfuture.com/russia-ukraine-cyber-front/>.

²⁹ Soldatov, Andrei and Irina Borogan. 2015. *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries*. PublicAffairs.

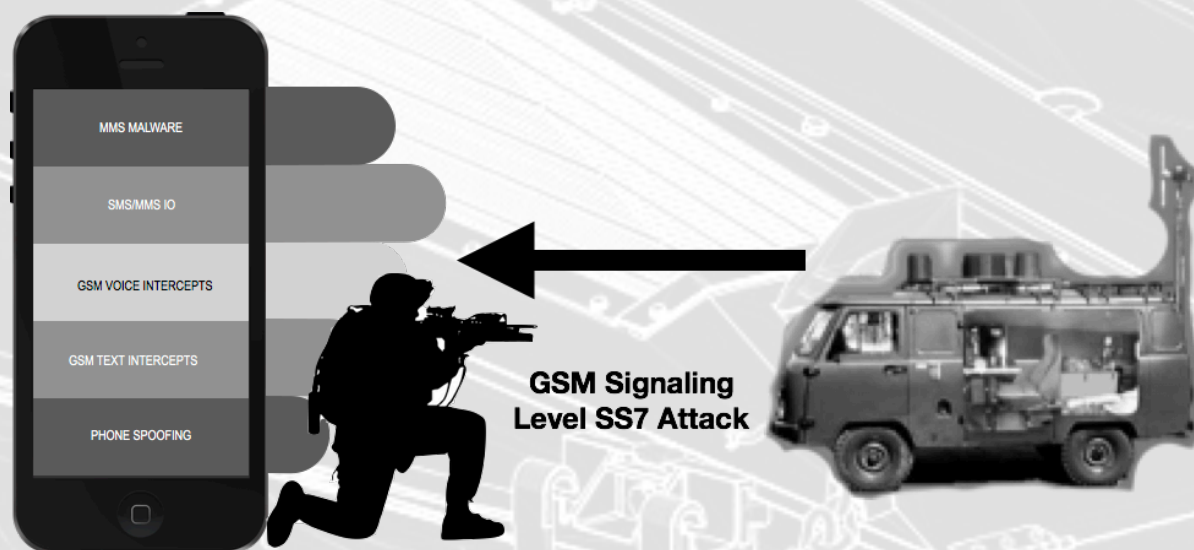
To manage this vulnerability, a military would have to eliminate the use of unencrypted communications within tactical level units. Although this can be accomplished and was indicated as a recommendation of the Ministry of Defense and the NSDC of Ukraine, our conversations with foreign advisors and soldiers from both regular units and volunteer battalions indicated that the use of personal, unencrypted communications was standard practice. When asked whether individuals were concerned for their safety in regard to use of insecure communications, the consistent response was “we still have to live.” The tradeoff between security and convenience within the Ukrainian conflict for soldiers operating within their own territorial boundaries was not surprising, but highlights a key problem in maintaining and protecting a young and developing military force in the face of a technologically adept adversary.

Based on our conversations at nearly every level, we identified a fundamental lack of training among Ukrainian soldiers on how Russia is exploiting their use of personal technology. Conscripts have posted geo-tagged selfies of themselves on the front lines on social media. While Ukrainian forces have improved their digital and signals security practices since the start of the conflict (as a result of painful lessons learned), a lack of training and poor communications discipline remain a key weakness of Ukrainian forces. Beyond training the consistency of improper personal security highlights an exploitation of insufficient within unit discipline and has been demonstrated to be a substantial roadblock to unit security. Many of those with whom we spoke indicated that the problem, while slightly diminished as volunteer battalions were replaced with regular units, has not entirely dissipated. The lack of sufficient communications equipment at the unit level made the use of clear communications through mobile phones and landlines a necessity, while communications at higher levels of command (battalion and above) had access to newer more secure communications equipment. Many of the former soldiers we spoke with indicate there was insufficient concern above the company level for the communications security of soldiers on the front lines. This lack of concern, is not entirely true, based on documentation received from the general staff, however, the problems of communication below the battalion level are acknowledged as insufficient at the present time. Thus, while higher levels of command were secure, the concern for the soldiers near the front was lacking or insufficient.



RP-377 Lorandit-AD Image Credit
RussianDefense.com

While some communications were compromised at the physical network level through the telecommunications providers, others were compromised through the interplay of the physical network layers of the telecommunications providers and a device's logical interpretation of the networks it was connecting to. Both forms of manipulation can achieve passive surveillance presence, and both forms can achieve active manipulation by elevating the attack from the network and logical layers to the cyber-persona layer. Both soldiers and military leaders indicated and provided evidence of not only passive surveillance but also sustained efforts to manipulate the cyber-persona layer for both IO and continued persistent surveillance when phones exited monitored network structures or went beyond the range of logical network spoofing capabilities such as IMSI-catchers or equivalents. Documentation provided to us by Ukrainian counterparts identified the primary technical equipment utilized by Russians to intercept and subsequently engage in GSM signaling attacks as the Russian RP-377L "Lorandit" (ELK-7077) mobile signals platform. Attacks using this system exploited Signal System No7 (SS7) vulnerabilities called the Common Channel Signaling System 7 (CCSS7).



Russian RP-377L "Lorandit" (ELK-7077) mobile signals platform SS7 Exploitation Explained

CCSS7 is a set of protocols that managed the connection of the phone to mobile networks. Targeted SMS and MMS messages were sent to soldiers and their families across Ukraine as a means of both achieving IO objectives and attaining persistent presence on devices within

proximity to the zone of hostilities and beyond. Additionally, once a persistent presence was achieved on devices indications point to the collection of contact lists allowing for further attack propagation.

Ukrainian forces have attempted to mitigate these vulnerabilities in a variety of ways. In some sectors of the ATO, in particular M-Sector, (the southern parts of Donetsk Oblast around Mariupol), Ukrainian forces have, based on interviews, turned to low-tech options such as semaphores (flags) and hardline telephone systems with unique wiring outside of SORM or using conventional wiring with encryption. Beyond technical and non-technical mitigation efforts both Ukrainian and Russian/separatist forces are using Military Deception (MILDEC) techniques on unsecure iCom communication channels (e.g. flooding and codewords). By contrast, Ukrainian forces in D-Sector (southern parts of Luhansk Oblast and eastern parts of Donetsk Oblast) were reported to have been provisioned with high-tech encrypted communications technology (256-bit encryption)³⁰ through private organizations such as “Army SOS,” a Ukrainian organization dedicated to volunteer provisioning of the Army.³¹ There were mixed reports on whether or not this technology had been compromised by Russian forces and we found no conclusive evidence either way.

In addition to leveraging novel forms of communications, military sources indicated a strong preference for satellite communications (SATCOM). SATCOM were believed to be more secure than mobile phones and landline communications. SATCOM were enabled mobility and communications without the needed training on Harris or similar radio systems. Although secure radio communications were possible via Harris or other similar system, the availability and training on these systems was not widespread.

In conversations with various groups associated with the Ukrainian military, tactical level units were noted to lack basic encrypted communications technology e.g. Harris Radios or other similar systems. Shortages of communications equipment were pervasive and we were told by soldiers that communications equipment was limited to approximately one radio per 350 personnel. Moreover, a substantial lack of funds forced many Ukrainian soldiers to use personally procured equipment including: cellular phones, Motorola iComs, laptops, etc. for command and

³⁰ 256-bit encryption is a data/file encryption technique that uses a 256-bit key to encrypt and decrypt data or files. It is one of the most secure encryption methods after 128- and 192-bit encryption, and is used in most modern encryption algorithms, protocols and technologies including AES and SSL.

³¹ <http://armysos.com.ua/en/>

control. In many cases, soldiers fighting along the ATO had to either purchase their own equipment and supplies or rely on the support friends and family. Two examples provided beyond communications procurement were the acquisition by soldiers of off-the-shelf hunting night scopes instead of night vision and body armor smuggled through Poland.

The diversity of devices within the military ecosystem at the tactical level and the variety of procurement avenues combine to make digital security extremely difficult. Even if all equipment were procured through official channels it is likely that digital devices would remain vulnerable. With the diversity of devices present, it is safe to assume many if not most are vulnerable to cyber-attacks of some form. The most common types of attacks noted were DDoS, SOCMINT, or man-in-the-middle attacks conducted using signals intercepts such as IMSI-Catcher equivalents. Although we did not find evidence of the manipulation of conventional weapon systems used at the tactical level, the manipulation of tactical level unit communications has resulted in substantial challenges. There were some indications of hacking unmanned aerial vehicles (UAVs) used by Ukrainians. However, during our discussions, we were unable to differentiate between cyber and EW attacks against UAVs, and therefore we group UAV targeting at the tactical level under tactical EW.

Throughout our discussions we found no current military based tactical cyber training program. The consistent response was that commanders do not know how to use or apply cyber effects or manage the cyber environment at the tactical level. Military cyber planners at the national level did indicate a draft plan for the creation of cyber personnel to be fielded at the tactical level, but they lacked the resources to implement this plan. Across our discussions we found a lack of consistency within the military and across the NSDC organizational structure for cyber planning and training for tactical level engagements. We also detected concern with certain groups that elements within the broader Ukrainian security infrastructure dominated cyber resource allocations, in particular the SBU. Our SBU counterparts indicated that unbalanced resource allocations, were *not* occurring and chalked up these concerns to typical political infighting with constrained budgetary cycles. However, when SBU personnel were not in meetings, we did receive substantiated indications that our concerns about imbalances of resource allocations within the security infrastructure were warranted. Irrespective of resource allocations there were no concrete short-term timelines for remediation of tactical cyber challenges absent approval through the NSDC, Presidential Administration and Verkhovna Rada. Documents provided by the MoD

highlight a robust conceptual development for sustained tactical, operational and strategic level thinking on cyber within the Ukrainian military. The “Cyber Defence System of the Armed Forces of Ukraine” which will be discussed in later sections offers a strong pathway forward for the development of a Ukrainian cyber defense force that includes tactical level goals and objectives for the development of both human capital and physical infrastructure requirements.

Despite multiple training missions from US National Guard units, the aggregate level of cyber security awareness and digital operational security was poor amongst soldiers. This is likely due to rapid force turnover and is unlikely to be mitigated in the short-term. Only select individuals maintained minimal cyber security awareness, although all expressed knowledge that their devices or communications were vulnerable. The lack of education and awareness challenges tactical level communications and the management of force structures. Awareness and education at the tactical level are further challenged by short force rotations and the loss of institutionalized knowledge over time.

Tactical EW

The US Army FM 3-12 released in April 2017 defines electronic warfare (EW) “as military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy.”³² Within Ukraine, there is substantial overlap between tactical cyber operations and tactical EW. This largely confirms the recent revisions to US Army doctrine within which cyberspace operations and EW are condensed into cyber electromagnetic activities (CEMA). The section above on tactical cyber differentiated those attributes by specifically focusing on the interpretation and manipulation of code-based structures or platforms, by contrast, this section focuses on the use of electromagnetic spectrum in particular the manipulation of that spectrum to achieve effects at the tactical level.

Beyond the manipulation or surveillance of digital devices via cyber means, EW incorporates the monitoring and disruption of physical network, logical or cyber persona layers, the use of EW to intercept electromagnetic (EM) emissions has proved extremely successful at the tactical level against Ukrainian forces. While tactical cyber looks at content, EW denies, degrades, manipulates or identifies the presence and measures volume. In discussions ranging from the

³² 3-12, F M. 2017. *Cyberspace and Electronic Warfare Operations*. Department of the Army.

NSDC to foreign advisors and soldiers, we received numerous reports of signals identification and subsequent triangulation for targeting. Triangulation is achieved through the identification of the existence of spectrum usage by an adversary. While SOCMINT might identify opposing forces through geographically tagged posts (geo-tagged) or content-based information on the position and movement of forces, EW at the tactical level targeted units to direct fires against Ukrainian personnel.

The use by Ukrainian forces of devices with EM broadcasting enabled adversary tracking of individual devices or volumes of devices within a given area. As devices broadcast EM signatures these are then used to identify where units are located within and their movements to the conflict zone.³³ The problem of EM control during the Ukrainian conflict was particularly pronounced in its early stages, this has been improved somewhat over the duration of the conflict and the professionalization of the military, yet remains a consistent challenge. Our discussions with members of the NSDC, military, soldiers and volunteers all confirmed what foreign advisors told us, that they have strong indications that Russian forces can intercept and access any and all EM transmissions at their discretion in the areas of conflict. Although reports from the Potomac Foundation indicate a substantial capability to deny communications, our discussions indicated that denial of communications was not the primary intent, rather the identification of communication volume and location of origin provided tactical advantages. The clustering of Ukrainian EM emissions in the early phases of conflict often led to targeting by Russian forces according to discussions with various parties. Rather than simply relying on imagery intelligence, the interception, analysis and triangulation of signals were indicative of massing forces and targeted fires could be directed against these positions. Although, reports indicate EW at the tactical level used to pre-detonate or dud incoming artillery and mortar rounds with electronic fusing, this issue did not come up in discussions of EW capabilities.³⁴ Because this topic did not arise we are unable to substantiate these claims. However, when asked about the major problems facing Ukrainian forces this issue was not mentioned.

The use of EW to both facilitate and counter unmanned aerial vehicles (UAVs), also referred to as drones, was discussed by members of the armed forces and foreign advisors. Drones

³³ Karber, Phillip, and Joshua Thibeault. 2016. "» Russia's New Generation Warfare" The Potomac Foundation. May 13. <http://www.thepotomacfoundation.org/russias-new-generation-warfare-2/>.

³⁴ Feickert, Andrew. 2017. "Selected Foreign Counterparts of U.S. Army Ground Combat Systems and Implications for Combat Operations and Modernization." Washington, D.C.: Congressional Research Service.

have been a substantial feature on the front lines of the ATO in Ukraine.³⁵ UAVs have been used by both sides in the conflict for surveillance, targeting and attacks.³⁶ UAVs are an inherently EM centric weapon-system and therefore highly vulnerable to EW. EM control via line of sight communications with the UAV and the use of GPS or alternative geospatial orbital tracking to provide location data are involved at the tactical level. UAVs form what Amos C. Fox refers to as a reconnaissance-strike model.³⁷ UAVs in Ukraine allow for consistent visual oversight on enemy positions as well as post fires battle damage assessments (BDAs). The variety and type of UAVs used in Ukraine on both sides of the conflict range from commercial off-the-shelf (COTS) quadcopters to custom fixed-wing long-range strategic surveillance craft. The diversity of UAVs and their combined uses with tactical movements in Ukraine has been the subject of numerous reports.³⁸ The use of UAVs in Ukraine by both Russian and Ukrainian forces in support of hybrid operations is novel, but what stands out in addition to the use of a new platform is the management of spectrum associated with the use of these systems.

In discussions with soldiers and representatives from Ukraine's army as well as foreign advisors, we identified substantial challenges faced by Ukrainian forces and Organization for Security and Co-operation Europe (OSCE) monitors in flying drones. UAVs were being targeted with a range of capabilities including surface-to-air missiles (SAMs), ZU-23 anti-aircraft guns, small arms, and jamming of communications and GPS.³⁹ Russian SAM and integrated air defense systems in addition to Krasukha-4 1RL257 ground-based EW platforms form part of the EW defensive mechanisms associated with tactical EW operations to counter Ukrainian UAVs. Air defense systems detect the flight of a UAV and provide targeting capabilities via SAM or other munitions, ground EW platforms jam or spoof the control or GPS signals associated with the maintenance of UAV position and flight. Combined Russian counter UAV strategies were found

³⁵ 2017. "Сбитый В Зоне АТО Беспилотник Оказался Российским Самолетом-Разведчиком 'Орлан-10'." *Unian*. Accessed October 10. <https://www.unian.net/politics/923698-sbityiy-v-zone-ato-bespilotnik-okazalsya-rossiyskim-samoletom-razvedchikom-orlan-10.html>; 2016. "Latest From OSCE Special Monitoring Mission (SMM) to Ukraine, Based on Information Received as of 19:30hrs, 8 February 2016 | OSCE." *Osce.org*. February 9. <http://www.osce.org/ukraine-smm/221436>; 2016. "Latest From OSCE Special Monitoring Mission (SMM) to Ukraine, Based on Information Received as of 19:30hrs, 15 April 2016 | OSCE." *Osce.org*. April 16. <http://www.osce.org/ukraine-smm/234151>; 2017. "Начальник Разведки 2-Го АК Под Контролем UCA. Part 1: БЛА 'Орлан-10' - InformNapalm." *Inform Napalm*. January 5. <https://informnapalm.org/31590-nachalnik-razvedki-2-ak-pod-kontrolem-uca-orlan-10/>.

³⁶ Mizokami, Kyle. 2017. "Kaboom! Russian Drone with Thermite Grenade Blows Up a Billion Dollars of Ukrainian Ammo." *Popular Mechanics*, July.

³⁷ Fox, Amos C. 2017. "The Russian-Ukrainian War: Understanding the Dust Clouds on the Battlefield - Modern War Institute." *Modern War Institute*. January 17. <https://mwi.usma.edu/russian-ukrainian-war-understanding-dust-clouds-battlefield/>.

³⁸ Friese, Larry. 2016. "Emerging Unmanned Threats: the Use of Commercially-Available UAVs by Armed Non-State Actors.." Armament Research Services; Ferguson, Jonathan, and N R Jemzen-Jones. 2014. "Raising Red Flags: an Examination of Arms and Munitions in the Ongoing Conflict in Ukraine." Armament Research Services; Bugriy, Maksym. 2014. "The Rise of Drones in Eurasia (Part One: Ukraine)." *The Jamestown Foundation*. June 23. <https://jamestown.org/program/the-rise-of-drones-in-eurasia-part-one-ukraine/>.

³⁹ 2015. "Rebel Drones: UAV Overmatch in the Ukrainian Conflict." The Foreign Military Service Office.

to be robust and effective against the limited budget on which Ukrainian forces were operating. Beyond merely countering the UAV threat, some individuals with whom we met indicated Russian capabilities to intercept and view Ukrainian UAV video feeds, thereby providing a tactical advantage to Russian forces.

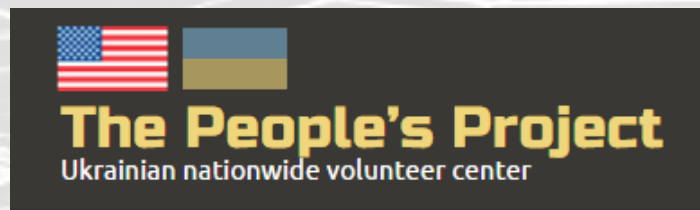
Discussions also indicated Russia has employed UAVs in the ATO to extend its capabilities throughout the Donbas region. Russia has used its UAVs for targeting, intelligence gathering, and as bait, waiting for Ukrainian soldiers to shoot as a trigger for an artillery strike. The Ukrainian army by contrast has generally been ineffective at targeting UAVs due to limited SAM/Air Defense assets and limited EW capabilities. The primary Ukrainian method of UAV engagement is small arms fire according to both senior military leaders, foreign advisors and direct accounts from Ukrainian service members. All noted small arms fire is inefficient and rarely effective. Former military members indicated that foreign-acquired holographic hunting sights purchased through civilian channels in third party nations improved small-arms effectiveness in countering UAVs. We found no evidence of EW counter-UAV systems being used by the Ukrainian forces. The use of UAVs for tactical advantage by Russian forces has included the control of Ukrainian movements along the contact line. Ukrainian soldiers within regular and volunteer Units noticed patterns of UAV overflights followed by directed fires from Russian positions. Soldiers this correlated the overflights to imminent threats against positions. This led Ukrainian personnel to take refuge in bunkers or other facilities. As these patterns of behavior gained regularity, it was noted by Ukrainian soldiers that Russian forces would use this opportunity to advance their positions forward.

Ukraine has deployed some individually-procured UAVs of their own, and there is some government production of UAVs for the Army through Ukraine's main defense contractor UkrOboronProm.⁴⁰ Other promising UAV production and development occurred through students at Kyiv Polytechnic and have, based on media, been deployed to the Ukrainian side of the conflict.⁴¹ Despite the development of UAVs on the Ukrainian side, there was widespread recognition among various groups that Ukrainian UAVs remained susceptible to interception, jamming, and spoofing. Media reports indicate that many units on the Russian sides of the line

⁴⁰ 2016. "UkrOboronProm Starts Supplying Drones to Ukrainian Army." *Unian*. January 26. <https://www.unian.info/society/1247198-UkrOboronProm-starts-supplying-drones-to-ukrainian-army.html>.

⁴¹ 2017. "New Drones Designed by KPI Students to Be Supplied to Ukraine Army." *Unian*. October 14. <https://www.unian.info/society/1224911-new-drones-designed-by-kpi-students-to-be-supplied-to-ukraine-army.html>.

including separatist units have access to the latest jamming and spoofing technologies from Russian suppliers.⁴² One interesting feature of the EW and UAV aspects of the conflict reported in the news and confirmed within our discussions was the societal approach to developing new technologies and provisioning Ukrainian forces. We were told of both hardware and software developers working on products for direct provisioning of Ukrainian forces. We also found indications of funding for the development of these tools both within Ukraine and extending into the diaspora through crowdfunding efforts such as the “People’s Project.”⁴³ The People’s Project raised \$41,633 to build multiple UAV platforms each with aerial surveillance and encrypted communications. Perhaps most interestingly, the project provided a public cost accounting of each dollar spent and where the final products were delivered. This is likely one of the first documented



cases of crowdfunding for a conflict and highlights the democratization of EW and UAV platform development and deployment within short production cycles.

Tactical Information Operations

Information operations have been used shape the tactical battlefield environment in conflicts dating back to Sun Tzu. In the recent campaigns in Iraq and Afghanistan campaigns, the use of IO has been widespread. While historical references to IO have been referred to under various terms ranging from psychological operations to information operations, the current naming convention refers to such operations in two distinct veins the first of which is Military Information Support Operations (MISO) defined as: “objectives to convince enemy, neutral, and friendly nations and forces to take action favorable to the United States and its allies.”⁴⁴

MISO is distinct from the second, tactical public affairs missions, which are defined as- “A process to coordinate and synchronize narratives, themes, messages, images, operations, and

⁴² Tucker, Patrick. 2015. “In Ukraine, Tomorrow’s Drone War Is Alive Today.” *Defense One*. March 9. <http://www.defenseone.com/technology/2015/03/ukraine-tomorrows-drone-war-alive-today/107085/>.

⁴³ <http://www.peoplesproject.com/en/bpla/>

⁴⁴ n.d. *Military Information Support Operations Command (Airborne)(Provisional) Fact Sheet*. U.S. Army Special Operations Command Public Affairs Office.

actions to ensure their integrity and consistency to the lowest tactical level across all relevant communication activities.”⁴⁵

The interaction of MISO and public affairs in tandem with efforts from tactical cyber and EW operations in Ukraine add to the complexity of tactical level operations. In particular the use of mobile phone and conventional radio intercepts via managed infrastructures (mobile providers, internet providers, SORM systems and other affiliated techniques) as well as the manipulation of device protocols to enable man-in-the-middle attacks to provide direct access to Ukrainian personnel has had demonstrable effects on the information environment at the tactical level. Documentation provided by the Ukrainian Information Assurance Directorate of the Main Signals Communications and Information (J6) of the General Staff of the Armed Forces of Ukraine gave insights into the tactical usage of mobile communications manipulations. Tactical level messages

“Your battalion commander has retreated. Take care of yourself.”

“You are encircled. Surrender. This is your last chance.”

“Ukrainian soldier, what are you doing here? Your family needs you alive.”

“You will not regain Donbas back. Further bloodshed is pointless.”

“Ukrainian soldier, it’s better to retreat alive than stay here and die.”

focused on the unit level and sought to alter the fighting capacity of frontline units. The quotes above detail several of the messages known to have been received by soldiers on the front lines.

We confirmed receipt of messages above and other similar with soldiers from both regular and volunteer Ukrainian units who served along the ATO. The impact of these MISO operations according to the soldiers that received them was the demoralization and significant consternation of Ukrainian forces. This was particularly the case as platoon to battalion level communications were, as demonstrated above insufficient, thus adding to the uncertainty of soldiers and stressing the trust between various levels of command.

Tactical level MISO operations directed against Ukrainian service members combined with robust public affairs within the Donetsk and Luhansk People’s republic have sought to shape the

⁴⁵ 2015. Joint Publication 3-61 Public Affairs. U.S. Department of Defense.

tactical environment on both sides of the contact line. While MISO operations have been directed against Ukrainian service members, Public Affairs operations and the restriction of access to various sites and services on the Internet within rebel and Ukrainian controlled areas of Ukraine have limited the breadth and expansiveness of the information environment. DNR and LNR administrative structures have both implemented Internet blacklists against Ukrainian and foreign media outlets online using a variety internet filtering techniques.⁴⁶ Blacklists limit the access of individuals within the LNR and DNR to news beyond the Rebel and Russian positions.

The public affairs mission within the rebel-controlled territories has been found to be a mix of white, grey and black propaganda and disinformation designed to harden support within the controlled areas against Ukrainian forces. Natalia Antelava, a BBC reporter in 2015 in an investigative report that found the structured and deliberate manufacturing of stories within the Donetsk People's Republic.⁴⁷ A Member of our team sat down with Antelava, who is now the head of Coda⁴⁸ and discussed the use of information operations in Ukraine. She indicated that the public affairs and psychological operations are deeply intertwined within the region and that the acknowledgement of reality and the establishment of the veracity of events was largely secondary to the controlled narrative of operations within DNR and LNR controlled areas.

Beyond meeting with members of the military, we also engaged faculty from Taras Shevchenko National University of Kyiv and the StopFake team at Kyiv Mohyla's Journalism School. While the approaches of faculty from both these Universities differed, both provided valuable insights into the complexities of IO operations both against the military and the wider Ukrainian society. Faculty from Taras Shevchenko highlighted the impact of the initial phases of IO on the ability of the Ukrainian government to mobilize and unify the nation in opposition to Russian activities in Crimea and the Donbas. Faculty indicated that the government had reached out to them to begin a process of understanding how to consolidate a national identity and counter IO operations from the Russian Federation. Moreover, they indicated the importance of fostering a unified national identity through the consolidation of television, print, and social media. They acknowledged concerns of the international community on the restriction of the freedom of the press and access to an unencumbered Internet, but countered by stating that any nation in a

⁴⁶ 2015. "Self-Proclaimed 'Donetsk People's Republic' Now Has an Internet Blacklist." *StopFake.org*. June 19. <https://www.stopfake.org/en/11796/>.

⁴⁷ BBC News: <https://www.youtube.com/watch?v=HW-4a0P8sis>

⁴⁸ <https://codastory.com>

sustained conflict environment with persistent external IO targeting against its citizenry and military would likely engage in the same counter-IO tactics. The efforts to limit the influence of foreign IO on the Ukrainian population has been remarkably successful and seen limited domestic opposition.⁴⁹ Conversations with local journalists and citizens reinforced what faculty at Taras Shevchenko indicated that the perception of an external IO threat and the necessity of laws and policies to counter that danger to societal unity. The tactical relevance of the larger strategic actions of banning Russian social media or limiting Russian broadcasts within Ukraine are not inconsequential and likely reduce the psychological impact on soldiers at the front line.

The StopFake project at Kyiv Mohyla and InformNapalm further add to the success of counter-IO operations in Ukraine across all levels.⁵⁰ The rapid contestation of IO within Ukraine limits the impact of general IO on Ukrainian soldiers and citizens. It provides a readily accessible source of counter-IO that is largely seen as credible. Journalists and citizens both cited these organizations as critical to helping counter aggressive information operations by the Russian Federation.

The counter-IO activities in Ukraine are generally thought of as successful, yet it is a challenge to continuously engage in counter-IO over the length of a long and sustained conflict. The duration of the conflict highlights a potential vulnerability identified by previous research on the topic of Russian IO that indicates sustained learning processes within the Russian Federation on the usage and implementation techniques to manage and alter perceptions within conflict zones.⁵¹ Russian planners and applied many of the lessons learned from previous conflicts, in particular Georgia to Ukraine.⁵² There is every reason to believe that sustained learning by the Russian Federation is still occurring as the volume and diversity of IO targeted against Ukraine and other nations continue unabated. Carmine Cicalese the former Director of the Joint Command Control, and Information Operations School at the Joint Forces Staff College notes that IO forms the critical link between actions and reactions and situational awareness and decision-making within the tactical environment. While IO can affect the psychological disposition of soldiers and their families at the tactical level it has proven impactful across all three levels and beyond within

⁴⁹ Sharkov, Damien. 2017. "Millions in Ukraine Flock to Facebook After Government Ban on Russian Websites." *Newsweek*. June 20. <http://www.newsweek.com/ukrainians-join-facebook-millions-russian-social-media-ban-627488>.

⁵⁰ <https://www.stopfake.org/>; <https://informnapalm.org/en/>.

⁵¹ Fitzgerald, Chad W, and Aaron F Brantly. 2017. "Subverting Reality: The Role of Propaganda in 21st Century Intelligence." *International Journal of Intelligence and CounterIntelligence* 30 (2): 215–40.

⁵² Iasiello, Emilio J. 2017. "Russia's Improved Information Operations: From Georgia to Crimea." *Parameters* 47 (2).

the broader citizenry of Ukraine and the international community. In the Ukrainian conflict at the tactical level the integration of Cyber and EW into IO operations has by most accounts created a potent mixture.

Tactical Cyber, EW and IO Advances and outcomes

It is important to state clearly that the cyber, EW, and IO effects at the tactical level while potent and damaging have not measurably altered the status quo of combined arms - force on force conduct. Although the additions of cyber, EW, and IO complicate conventional tactical-level activities, they have not altered the ability of one side or another to break significant deadlocks between forces. The current status quo of low-level hostilities between Ukrainian and Russian forces is likely not the result of the addition of these tools and tactics to conflict. Conventional force on force capabilities at the tactical level remain the most significant factor in determining battlefield success.

The inability to leverage these new tools and tactics to achieve substantial tactical success is best differentiated between the Ukrainian and Russian positions. While not altering the outcome of the conflict or creating a victory for one side of the other, the combination of cyber, EW, and IO at the tactical level have likely reduced the necessary scale of Russian intervention. The employment of these tools has facilitated relatively small force structure of Russian soldiers Russian who are able to maintain robust control over disproportionately larger territories. The hybrid tools have in essence increased the efficiency of maintaining a toehold in Ukraine at relatively low cost.

By contrast, these tools have increased the relative costs to the Ukrainian side of the conflict by making communications and control of forces at the tactical level more difficult. The combination of EW and cyber with IO have and continue to challenge Ukraine's tactical environment. Although Ukraine is rapidly developing the innovative skills and techniques to combat the tactical level manipulations these adjustments to an adversary are ongoing and unlikely to be mitigated quickly or significantly impact on conflict outcomes.

Cyber, EW, and IO at the Operational Level in Ukraine

Joint Publication 3-0 on Joint Operations defines the operational level as that which links tactical employment of forces to national and military strategic objectives.⁵³ This definition is somewhat unsatisfactory as it glosses over what Edward Luttwak describes as the location where “the schemes of warfare, such as blitzkrieg or defense and depth evolve or are exploited.”⁵⁴ Here the focus is on the planning and development of force structures to accomplish tactical level activities in pursuit of strategic goals. While the strategic level of warfare establishes the ideas, and synchronizes elements of power to achieve theater, national and/or multinational objectives,⁵⁵ and the tactical level focuses on the movements and plans to execute battles and other activities to achieve specific military objectives, the ability to carry out the tactics are derived from operational level through training, planning, organization, acquisition and allocation of resources. It is important to note that actions occurring at the strategic, operational and tactical level do not necessarily happen in discrete phases. Rather the three levels interact and provide overlapping feedback loops through concurrent actions.

The operational level of the Ukrainian conflict is rife with challenges. This section focuses on the training of personnel and the development and acquisition of resources that enable implementation of strategy at the tactical level in Ukraine. Allocation of resources was largely highlighted at the tactical level in the previous section and will not be included here. However, it is important to note that a failure to receive adequate resources at the tactical level results from failures that emanate from operational and strategic level issues.

Training

The ability to engage in and counter cyber, EW and IO at the tactical level necessarily begins with training at the operational level. The ability to develop the skills and plans necessary to engage an enemy utilizing new technical implementations can and often does happen at the tactical level, but doing so creates an ad hoc response that is unbalanced across tactical formations. This has been the case in Ukraine. As illustrated in our analysis of the tactical level, the distribution

⁵³ 2011, “Joint Publication 3-0 Joint Operations.” U.S. Department of Defense.

⁵⁴ Luttwak, Edward N. 2017. “The Operational Level of War.” *International Security* 5 (3): 61–79.

⁵⁵ 2011, “Joint Publication 3-0 Joint Operations.” U.S. Department of Defense.

of skills and resources widely diverges across individuals and units and creates imbalances and weaknesses that can and should be corrected at the operational level.

Over the course of meetings and discussions in Ukraine with members of the General Staff and the SBU, those with whom we met identified an urgent need for training. Many of the requests made of our group involved training resources or materials. Ukraine's training needs are extremely diverse at the operational level. Ukraine currently divides its cyber responsibilities across six government structures. Here we will focus on three of the six organizations: The Ministry of Defense, the Security Service of Ukraine, and the National Cyber Police.



Information Assurance Directorate of the General Staff of the Armed Forces of Ukraine (IAD)

The current staffing levels of cyber defenses Ukraine's MoD could be at best considered low. The inability to pay and train individuals within the Ukrainian armed forces in the fields of cybersecurity and electronic warfare is a direct result of inadequate funding caused both by bureaucratic friction and by economic vulnerabilities highlighted above. Ukraine's current plans for military-focused training has led to substantial confusion as NATO currently funds a variety of projects designed to raise level of human capital and network defenses of Ukraine.⁵⁶ NATO funding provided under a comprehensive assistance package for Ukraine (CAP) was endorsed in July of 2016. The initial budget of this fund was just under one million USD. We found that the resources provided by NATO were not making their way to the MoD, but rather remained largely with the domestic security services. The decision to utilize the efforts for security rather than within the ministry of defense was perceived by some with whom we spoke as damaging to the effort to establish robust training. There are indications that alternative international funding sources might become available in the coming months.

MoD IAD personnel provided information indicating substantial continued interest in basic cyber hygiene within the Ukrainian forces. Much of the training has been conducted by National Guard elements under a security awareness training program initiated in 2013 and continued on a

⁵⁶ 2016. *Ukraine Cyber Defense Fact Sheet*. North Atlantic Treaty Organization.

periodic basis.⁵⁷ Trainings have been conducted with support from EUCOM, the California National Guard, Marshall Center, Czech Cyber Center, and NATO. Trainings have included information on cyber hygiene and consultations on defensive strategy and processes to enhance cyber defenses and network security. The distribution of these resources beyond a core group of individuals within the IAD limits the breadth of impact and might lead to potential losses if key members of the IAD leave the military.

Consultations and advising on cyber defense appear to be paying off. The IAD provided us with documentation of proposed instructor preparation for tactical level cyber. The course sketches are robust and begin what is likely to be a long process of enhancing the cyber capabilities of the Ukrainian Army. Currently initial training is directed towards creating instructors with basic skills and comprehension of data exfiltration, signals and cyber manipulation in conflict areas and beyond, the confidentiality, integrity and availability (CIA) triad and the development of a variety of network and host defensive skills relevant to the tactical level. More advanced course descriptions for forensic and audit analysis of networks are also under construction. These courses educate trainers to expand capacity. After initial training capacity is developed the skill-sets will then be extended outward.

At present the Ukrainian military lacks the resources to provide the necessary technical certifications, training exercises, and physical tools required to counter – or even mitigate – the Russian threat. Currently, the Army's General Staff seemingly relies on the efforts of one well-educated, visionary, and highly over-worked field grade officer to develop its entire cyber defense strategy. The operational level of cyber and EW within the Ukrainian MoD IAD is progressing within the constraints and vulnerabilities outlined in previous sections. The leadership responsible for the continued development of these programs were trained in U.S. graduate school programs and have what can only be described as a sense of purpose and a mission. This sense of purpose and mission are essential in a difficult resource and bureaucratic environment.

⁵⁷ Everfield, Carlos. 2013. "Security Awareness and Developing a Cyber Workforce." *Eucom.Mil.* January 5. <http://www.eucom.mil/media-library/blogpost/24884/security-awareness-and-developing-a-cyber-workforce>.



Security Services

The competency of the Security Services of Ukraine has increased markedly in recent years as it has shed much of its former senior leadership. Individuals with whom we met indicated that following the departure of President Yanukovych the executive offices of the SBU were left hurriedly in a state of disarray. The new cadre of officers and senior leaders seemed, within our meetings, to be extremely concerned about the security and resilience of the Ukrainian state in the face of Russian aggression. However, security services in post-Soviet countries often remain intimidating to many other government institutions and Ukraine is no exception. In most meetings in which representatives of the SBU were present, they led conversations and discussions and afforded little room for dissenting views that were at times expressed while walking to or from meetings. Based on our understanding and interpretation from a variety of sources, the SBU has taken a central role in facilitating Ukraine's cyber defense. In meetings with SBU cyber leadership they strongly expressed a desire to promote joint efforts across the nation. The SBU's operational level capabilities are important in facilitating and maintaining tactical level capabilities, particularly in a country where the conflict is occurring on its own soil.

NATO's Trust Fund on Cyber Defense for Ukraine has been robustly leveraged by the SBU and coordinated across other institutions within the cyber defense mission of Ukraine, notably the State Special Service of Special Communications and Information Protection. Based on our conversations with both members of the SBU and MoD, the majority of external funds for cyber defense have been used to train individuals or organizations affiliated with state security. Although this might appear on the surface to be bureaucratic land grab against the MoD, the SBU's logic is that the operations occurring within Ukraine are defined as terrorism related and are therefore directly relevant to their mission of fighting terrorism and espionage.

Although our group did not have direct access to training facilities we did make substantial inroads with the Kyiv Polytechnic Institute (KPI) which indicated partnerships with the security services and training of future officers. Unlike in the MoD where we were able to review a

consolidated and robust proposed pipeline for training and capacity development, we did not receive any such documentation from either the SBU leadership or KPI affiliates.

The level of passion for cyber and EW issues was not as prevalent within the meetings with SBU and SBU-affiliated KPI personnel. Both groups were professional and interested in expressing their concerns over Russian aggression, seeking additional financial and training resources to advance their mission. Although our initial impressions of SBU personnel diverged markedly from those of the MoD this is likely a function of culture between organizations and does not express an unwillingness to develop training or remediation strategies to the challenges faced by Ukraine.



National (Cyber) Police

Although not directly related to military or national security aspects of Ukraine the National Cyber Police highlight what might be considered the single most successful training and organizational pipeline for cyber related issues in Ukraine. While we also did not receive direct access to their training documentation, our discussions on their development process and their

...the National Cyber Police highlight what might be considered the single most successful training and organizational pipeline for cyber related issues in Ukraine.

nation-wide staffing and allocation timeline indicate substantial progress. The first group of 84 cyber-police officers were funded by OSCE at Kharkiv National University. Each of the 20 special agents and 64 officers participated in a 760-hour training curricula that took place over four months. The first class of cyber officers graduated on July 18, 2016.⁵⁸ In their presentation to us they indicated a measured schedule of development of cyber police capabilities across the nation. The cyber police are a generally transparent area of success that offer a model for foreign engagement in Ukraine.

⁵⁸ 2017. "OSCE-Trained Ukrainian Cyber-Police Officers Begin Fulfilling Their Mission | OSCE." *Osce.org*. Accessed October 19. <http://www.osce.org/ukraine/254761>.

Combined the training attributes of the MoD, SBU and National Police indicate progress towards enhanced cybersecurity. The training progress is strained by limited human capital and financial resources spread across different institutions. Each of these institutions, when questioned on the extent of training, universally indicated that all training and development was being structured solely to establish defensive security within Ukraine or for criminal investigative purposes for crimes occurring in Ukraine.⁵⁹ Pressed further, they each indicated unequivocally no desire to engage in offensive cyber operations of any kind. Their focus on defensive cybersecurity and their different missions codify, at the operational level, a broad governmental approach to enhancing capacity and capability oriented towards the defense of Ukraine.



Development and Acquisition of Resources

Linking the strategic and tactical levels, the operational level necessarily includes the development of the tools and the provision of resources needed to conduct operations at the tactical level. Ukraine is in many ways unique in its concentrated efforts to manage the development and acquisition process due to the highly consolidated defense industrial base. While in Ukraine, our team met with members of UkrOboronProm, an association of multi-product enterprises spanning sectors the national defense industrial base. Although discussions with UkrOboronProm focused on cyber, EW, and IO, it is necessary for a broader context of the association and its role in Ukrainian and Russian defense is necessary.

UkrOboronProm is the result of a 2010 reorganization of Ukraine's defense industrial base (DIB) following the election of President Viktor Yanukovich in 2010. The consolidation of Ukraine's DIB brought numerous corporations into a unified organizational structure. From 2010 until 2014 UkrOboronProm maintained deep financial and structural ties both within Ukraine and Russia.⁶⁰ Large swaths of the DIB were located in the eastern portions of the country now currently

⁵⁹ There is little to no emphasis placed on cybercrimes occurring against international entities that originated in Ukraine.

⁶⁰ Arbatov, Alexei, and Vladimir Dvorkin. 2014. "Close Ranks." *Foreign Affairs*, May.

embroiled in conflict. From 2012 to 2016, UkrOboronProm was the world's ninth- largest arms exporter with estimated revenues over \$6.9 billion.⁶¹ A 2016 RAND report on security sector reform in Ukraine highlights many issues that became evident in our discussions with UkrOboronProm staff and leadership. First, a consolidation of military contracting and

TRAINING AND EDUCATION ACHIEVED THROUGH MILITARY SERVICE, PROFESSIONAL SCHOOLING, HIGHER EDUCATION OR OTHER FACILITIES FUNDED BOTH THROUGH UKRAINIAN BUDGETS AND EXTERNAL FINANCIAL AID APPEARS TO BE SUBSEQUENTLY TRANSFERRED TO PRIVATE ENTITIES WHO THEN WISH TO CHARGE THE STATE FOR SERVICES RENDERED.

procurement within the DIB leads to higher prices and lower quality.⁶² Second, the consolidation of the DIB limits competitiveness, challenges transparency and reduces efficiency.⁶³ Third, and most importantly for the field of cybersecurity is it provides direct financial challenges to government and military cyber capabilities through the creation of organizational structures suited to the outsourcing of core government responsibilities within cyberspace, namely the development of Computer Emergency Response Teams (CERTs). Fourth, due to its overarching control over the DIB within Ukraine it has a significant disincentive to procure products that might be produced by its subsidiaries irrespective of strategic goals and tactical needs.⁶⁴ Simply put, the consolidation of the entirety of the DIB under UkrOboronProm creates operational level inefficiencies by following what RAND scholars argue is a Soviet Era Hybrid structure. Combined the current Ukrainian DIB has the potential for corruption, inefficiency, and poor outcomes.

Despite many of the issues listed above, UkrOboronProm and in particular its subsidiary Ukrinmash, do have highly talented individuals in cybersecurity. Prior to our arrival Ukrainian teams from the Ukrainian C4ISR Centre of Ukrainian Armed Forces won two of the three competitions at 2nd Enterprise Architecture Hackathon sponsored by NATO.⁶⁵ Many of the individuals from these two teams subsequently left the Ukrainian military and joined Ukrinmash to help the subsidiary in the formation of a quasi-public-private CERT. When questioned on why they left the armed forces these individuals indicated that salaries for highly skilled individuals on

⁶¹ Menon, Rajan, and William Ruger. 2017. "The Trouble with Arming Ukraine." Foreign Affairs, October.

⁶² Olikier, Olga, Linn E Davis, Keith Crane, Andrew Radin, Celeste Ward Gventer, Susanne Sondergaard, James T Quinlivan, et al. 2016. "Security Sector Reform in Ukraine." Rand.org.

⁶³ Ibid.

⁶⁴ Ibid.

⁶⁵ 2017. "Final Report: 2nd Enterprise Architecture Hackathon ." *Act.Nato.Int.*

the Ukrainian UA-CERT started at approximately \$200/month, far lower than comparable salaries in the private sector. The result was the cannibalization by the sole Ukrainian Defense contractor of national capabilities. When further probed on this topic, Ukrimash leadership indicated that the development of a public-private CERT in Ukraine would allow them to respond to state needs while still earning financial returns. The transfer of human capital from state entities including the armed forces and security services to the private sector is not unique to Ukraine, however, it is particularly pronounced and damaging to the development of state-based capacity.

Training and education achieved through military service, professional schooling, higher education or other facilities funded both through Ukrainian budgets and external financial aid appears to be subsequently transferred to private entities who then wish to charge the state for services rendered. The general facilities and infrastructure within Ukrimash were far superior and more conducive to the retention of young trained cyber experts than comparable governmental facilities. When questioned on what resources were needed to assist Ukraine in the current conflict, Ukrimash leadership requested material resources including equipment, software and training.


While the Ukrainian Armed Forces, Security Services and National Cyber Police train and develop personnel at the operational level for discrete tactical environments, Ukrimash is subsequently hiring many of these individuals. Although Ukrimash provides further training and financial opportunities, the end result is a DIB with human capital that begins to exceed that of the state in cyber defenses while at the same time attempting to sell that defense back to the state.

The acquisition of EW equipment and the development of IO and EW systems within UkrOboronProm were not discussed in any of our conversations. While the tactical EW section above did include information on the development of UAVs our counterparts did not discuss the development of these capabilities.

The Operational Impact

The development of training and acquisition of resources has formed the centerpiece of international efforts to engage Ukraine. While many of the training efforts are largely uncontroversial, the provision of weapons to Ukraine for defense or offense has been extremely controversial.⁶⁶ The provision of physical hardware for the purposes of counter cyber, EW, or IO

⁶⁶ Walt, Stephen M. 2015. "Why Arming Kiev Is a Really, Really Bad Idea." *Foreign Policy*. February 9. <https://foreignpolicy.com/2015/02/09/how-not-to-save-ukraine-arming-kiev-is-a-bad-idea/>.

A detailed technical line drawing of a mechanical assembly, possibly a piece of electronic equipment or a vehicle component. The drawing shows various parts, including a large rectangular panel with a grid of small circles, a circular component with a central lens or opening, and various structural frames and supports. The drawing is oriented diagonally across the page.

is likely of limited utility absent the provision of training on how to use and maintain systems and networks from the tactical to the strategic level. Unless organizational structures are institutionalized and personnel turnover is minimized, the provision of physical assets are likely to be under or improperly utilized and would therefore create further problems. Current engagements through EUCOM, NATO, the EU, and OSCE among others that establish training pipelines, foster standardization and institutionalization within the armed forces and security services are likely to have more substantive lasting effects on the ability of Ukraine to defend itself against cyber, EW and IO. Further work with the EU to increase government capacity and transparency is further likely to reduce interagency rivalries and reduce corruption. Combined this will increase the resilience of Ukraine in the face of sustained external hostilities far more than the provision of any single piece of equipment.

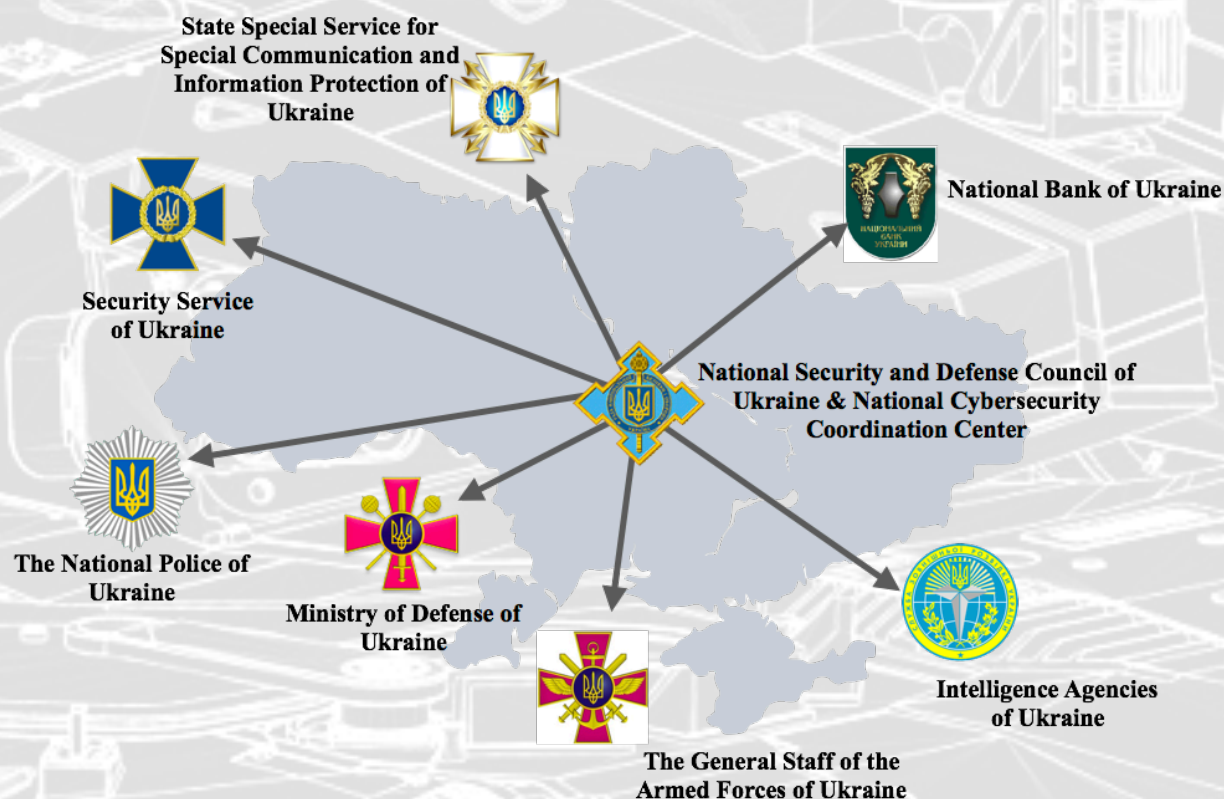


Figure 1: Ukrainian National Cyber Security Coordination Structure

The Strategic Level of Cyber, EW, and IO in Ukraine

The tactical and operational levels highlight issues relevant to the prosecution of conflict in Ukraine and offer insights to those activities and resources affecting soldiers and operators. The strategic level according to JP 3-0 Joint Operations establishes ideas for employing the instruments of national power in a synchronized and integrated fashion to achieve theatre, national, and or/ multinational objectives.⁶⁷ In the context of Ukraine - strategy includes the development of laws, policies, organizations and structures to counter or engage in hybrid warfare. Because hybrid warfare in the context of Ukraine is societal, the examination of the strategic level of hybrid conflict in Ukraine from the context of the military is limiting. Despite its limitations, the challenges faced by the Ukrainian military and by extension Ukrainian society are not entirely dissimilar. The requested policies and law changes that would affect the prosecution of conflict highlighted and are fed directly by challenges at the tactical and operational levels and many of

⁶⁷ 2011. "Joint Publication 3-0 Joint Operations." Department of Defense.

these same challenges arise in similar forms within civilian sectors in Ukraine, albeit with different effects and consequences.

Ukraine's Strategic Documentation Hierarchy



Figure 2: Hierarchy of Ukrainian Strategic Documentation

In discussions and from documentation received from the General Staff we noted a robust effort on behalf of the General Staff and the Security Services to rapidly engage the Verkhovna Rada and the presidential administration in legal and policy changes that would alter the resource allocations, organization, operational and tactical abilities of Ukraine in the current conflict in eastern Ukraine.

The structure of strategy for military related cyber, EW, and IO is subordinate to a hierarchy of laws starting with the Constitution and running through the National Security Strategy of Ukraine, to the Cybersecurity Strategy of Ukraine, and the Annual Plan for Cybersecurity Strategy. This structure attempts to place cyber related issues within the broader Ukrainian national security framework. The National Security and Defense Council of Ukraine has a coordination committee focused on cybersecurity which involves seven primary entities, of which the Ministry of Defense is one. See Figure 1 for the National Cybersecurity Coordination structure under the National Security and Defense Council of Ukraine.

The national cyber strategy of Ukraine (Стратегія кібербезпеки України) from March 15, 2016, places an emphasis on the development of cyber defenses in Ukraine. Yet the responsibilities for cyber defense are divided amongst various parties within the National Security

and Defense Council. The duties allocated to the MoD are restrictive and conflicting in Ukraine and likely serves as the basis for much of the inter-organizational friction we witnessed. The MoD is tasked with carrying out measures to prepare the state to address aggression in cyberspace (specifically through cyber defense) and the implementation of military cooperation with NATO. It is tasked with carrying out this defensive mission in cooperation with the State Service for Special Communications and Information Protection and the Security Service (SBU) of Ukraine.⁶⁸ The MoD is specifically responsible for “competence - to carry out measures to prepare the state to reflect the military aggression in cyberspace (cyber defense).” However, the current definition of hostilities in Ukraine constrains the MoD due to the conflict being designated as an anti-terror operation. This designation constrains the ability of the MoD to secure resources and places it in direct competition with the SBU, whose responsibility includes counter-terrorism.

There is recognition across most of the NSDC cyber entities and in particular within the IAD that the current national regulatory frameworks, technical standards, manuals and guidelines for IA-CD within Ukraine are inadequate. The current basis for technical standards that arose within discussions are US National Institute of Standards and Technology (NIST) special publications. Although NIST special publications are robust they are generally inadequate within the organizational, legal, technical and regulatory structures of Ukraine. To implement NIST standards and policies many other regulatory and legal frameworks are necessary within Ukraine that will enable NIST implementation. The lack of national level frameworks and policies to facilitate IA-CD hampers efforts at improving MoD and other government networks in the face of sustained external threats. While IAD documentation notes these inadequacies, conversations with other agencies indicate a universal recognition of the problem and a desire to address and remediate these shortfalls.

Most of the NSDC organizations recognized a general lack of awareness of cyber security culture within Ukraine. Despite sustained attacks against critical infrastructures in Ukraine and attacks against governmental and non-governmental entities there has been generally slow progress on policies, laws and public awareness campaigns to promote a culture of cybersecurity awareness. This problem is particularly pertinent and pervasive within the military and extends across all levels. Beyond a general lack of awareness of the importance and need for security among the rank-and-file there is a broad recognition within the IAD that the information assurance

⁶⁸ See section 3 of Стратегія кібербезпеки України. <http://www.president.gov.ua/documents/962016-19836>

and cyber defense (IA-CD) capabilities of the MoD have severe inadequacies within its organizational and command structure. The current IA-CD operations of the Ukrainian armed forces are staffed with less than 50 persons. These 50 persons are responsible for securing the network equipment associated with more than 250,000 personnel. By even the most modest information assurance and cyber defense standards this would be considered severe understaffing. The Ukrainian military has an approximate ratio of 1 to 5000 whereas the US army has an estimated ratio closer to 1 to 300 IA-CD trained or equivalent personnel.⁶⁹ The US also has the ability to surge an additional 13 national guard and reserve battalions. The comparable industry standard is approximately ranges between 1 to 50 and 1 to 500 based on automation, industry and efficiency. This begins to highlight many of the challenges that occur at the operational level and exacerbates conflicts between the military, security services and defense contractor over financial resources and human capital. It further highlights the challenges faced at the tactical level. Currently, the cyber defense division is concentrated within Kyiv, although other facilities are planned or in the process of being formed within Odesa, Rivne and Dnipropetrovsk.

Documentation from and discussions with the General Staff indicates the following sources or causes of problems associated with IA-CD in Ukraine's Armed forces: **1)** repeated reduction of funds to develop forces; **2)** constrained military authorities; **3)** underestimation of the value and importance of IA-CD activities; **4)** fragmentation and duplication of efforts across military units, **5)** lack of professional development and career enhancement paths; **6)** inability to retain personnel due to "brain drain" to civilian jobs in security organizations/firms.

The six challenges identified above are substantial and reflect many of the economic and bureaucratic challenges faced by the MoD in the current conflict environment. However, it should be noted that despite the difficulties the MoD of Ukraine has established a robust and detailed timeline for the remediation of many of the challenges listed above extending from 2017-2020. Remediation planning includes familiarization with NATO/US partners capabilities and infrastructures, development of training pipelines and capabilities, collaboration and engagement with partners on programs and projects to elevate Ukrainian skills and capacities. Included within the MoD are substantial plans to develop vigorous partnerships that will enable IAD personnel to contribute to programs with various partners. These contributions include the creation of


⁶⁹ Estimated value based on number of estimated personnel at ARCYBER (1,500) and 11 active signals battalions (~300/battalion comprised of 1 HHC, 2 ESC, 1 ASC) and current US Army personnel level of 1,340,000 as of October 31, 2017.

information sharing capabilities, joint cyber incident response and mitigation procedures, vulnerability management procedures and more. The IAD seeks develop capacity while managing interoperability within NATO standards and procedures.

In tandem with integrating and developing current IAD capabilities the IAD seeks to establish a robust program professional development. To accomplish this, at present the IAD appears, *on paper*, to be heavily reliant on NATO partners, in particular organizations such as the US Army Cyber Center of Excellence, Naval Postgraduate School, Marshall Center and private partners. Current planning on professional development highlights skill and capacity development but seems to lack career management within the MoD and will likely result in the short-term development of highly skilled individuals who will have little long-term incentive to remain within the Ukrainian military other than the prospect of further professional development opportunities. Although professional development is vital to the development of IAD capabilities, professional development in the absence of a career development pipeline is likely to lead to rapid turnover and inconsistent capability maintenance. There was a recognition of the need for career tracks that encourage individuals to remain in the Ukrainian Armed Forces, but on paper these same goals are inadequately expressed.

Documentation provided to our team indicates a 3-year timeline for the development, upgrade and acquisition of IA-CD systems and infrastructure. As highlighted several times above the current infrastructures, particularly at the company level and below are lacking. While documentation indicates a desire to start at the “operational” or “command post” level and higher within the next 12 months, the development of similar capabilities at the tactical level are likely to be slow and drawn out over 36 months extending to 2020. Both objectives are likely to be constrained by the fiscal realities of Ukraine and external partner willingness to fund activities beyond training.

Beyond IAD integration and capability development is a desire to provide a potent assessment and advisory capability for the MoD and the nation. The IAD expressed both in documentation and in discussions a desire to be involved in the broader discussion within Ukraine on the structure, organization, and utilization of the MoD for cyber defense. The elevation of IAD voices within the MoD and beyond to the Verkhovna Rada and Presidential administration is uncertain and is likely to be constrained by other competing interest within the NSDC cyber committee, in particular, the security services.

A detailed technical line drawing of a mechanical assembly, possibly a vehicle chassis or a large piece of machinery. The drawing shows various components like a central platform, wheels, suspension, and structural beams, all rendered in a clean, technical style with white lines on a light gray background.

The strategic environment for cyber, EW, and IO in Ukraine is not limited to military or security service challenges, but rather extends across the entirety of society. Many of the economic vulnerabilities listed in Part II challenge strategic level planning through constrained financial and human capital resources. Many of the challenges faced by the military are directly applicable and parallel the challenges faced across every sector of Ukraine and within its government. General cybersecurity awareness, legacy infrastructure, corruption, and human capital flight require more than short term fixes. While piecemeal solutions can be attempted the ability to counter hybrid conflict likely will require a whole of society effort, supported by external partners, in particular the EU and NATO to promote reasonable laws and policies that make the strategic, operational and tactical environments more defensible. The challenges described in the sections above are compounding and symptomatic of problems faced across nearly every institution in Ukraine. Part IV below posits several general recommendations predicated on our research findings.



Recommendations

Hybrid conflict involving the use of cyber, EW and IO operations are a mainstay of the conflict in Ukraine and are likely to be a prominent feature in all future conflicts. The use of cyber, EW, and IO in Ukraine offer a glimpse at some of the novel ways in which technology is impacting the conduct of the conflict. These tools in isolation are unlikely to provide substantial tactical, operational or strategic benefit or detriment to either an aggressor or defender in a given conflict, however, when used in concert with other instruments of diplomatic, military and economic power they combine to form a potent and pervasive challenge. This challenge affects every level of society and institutions of state. In states with limited or developing institutional and organizational capacity, even in the absence of pervasive digitally dependent weapon systems, the use of hybrid warfare means of conflict are particularly potent. Novel threats challenge weak institutions ability to adapt to or resist threats. Ukraine serves as a case study of a country building institutions and structures to confront hybrid challenges in real-time. The successes of Ukraine are not to be understated. It has successfully maintained a reasonably democratic state and institutions despite sustained aggression on its territory. It has created institutions such as the National Security and Defense Council and combined organizations within its bureaucracy in an effort to confront external challenges. While there are substantial interagency tensions, these tensions are playing out within a system of governance that has to date resisted and external efforts to cause chaos.


The military has risen to the challenge form a physical defensive barrier to safeguard most of the population of Ukraine. It has done so after years of neglect and corruption. The current status of the military while imperfect has accomplished remarkable results. The incorporation of volunteer battalions into a regularized force structures stands out as a success story that could have resulted in extremely deleterious effects for the country. The reorganization and standardization of processes within the military are incomplete. Partnerships with NATO, EUCOM, OSCE and a host of other organizations will continue to impact and provide much-needed guidance on areas in which improvements are needed.

The development of the Security Services, National Cyber Police, and other organizations under the NSDC focused on cyber within the last three years is nothing short of astounding organizationally and intuitively within the post-Soviet space and serves as a testament to the resilience of the Ukrainian people and their desire to maintain an independent democratic state. While this report focused on a single set of issues, the broad scope of issues being addressed across the country is immense and encompassing. Although many Ukrainians would like the process to occur much more quickly, the pace of change is steady, and the trajectory is largely in the right direction. To continue to build upon the achievements achieved since 2014 we present five core recommendations related to the scope of this report below with three focused on domestic actions, and two focused on international actions:

First, the development of cyber, EW, and IO skills for countering aggressive actions from the Russian Federation will only be successful if institutions develop within legal and policy frameworks that foster clarity on roles and responsibilities, between agencies and organizations within Ukraine and encourage and foster interagency collaboration and coordination. In particular, better collaboration and coordination is vital to the security services and the MoD. Clarity of responsibilities and roles between these two organizations will foster a workforce that will become mutually reinforcing and work toward the mutual defense of the nation. Increased collaboration and coordination will also reduce potential areas in which corruption might occur and thereby increase trust in Ukrainian institutions.

Second, there is a clear need to foster not only the career development through increased education but through advancement and remuneration. Although there will always be a financial imbalance between public and private sectors, the divide at present is likely to make sustained defenses in cyberspace, electronic warfare and information operations untenable. Establishing career tracks for officers and enlisted personnel and allocating financial resources to keep them in the service of the Ukrainian state for longer durations is likely to result in the institutionalization of knowledge and processes that foster the physical and economic security of the nation over the long haul.

Third, prioritizing national cybersecurity awareness through laws, policies, regulations, and domestic information campaigns is critical to increasing societal resilience and security in the face

A detailed technical line drawing of a mechanical assembly, possibly a vehicle chassis or a large piece of machinery. It shows various components like beams, bolts, and a circular component, all rendered in white lines on a gray background.

of a sustained external threat. While NSDC institutions are building capacity, elevating national cyber resilience will ease the burden these organizations face. Cyber hygiene within the government, public and private organizations and in particular among soldiers at every level is likely to reduce aggregate vulnerability and enhance public safety and national security.

Fourth, the international community should continue to engage Ukraine. Emphasis should be placed not only on training and providing resources but on the development of institutional and organizational capacity and structures to retain, support and maintain individuals who are trained within the military, the security services and the National Cyber Police.

Fifth, continued research on the evolution and utilization of cyber, EW, and IO occurring at all levels within the Ukrainian conflict extending from the ATO to the broader society should continue. The evolution of tactics, techniques and procedures created by the learning environment available to the Russian Federation and its proxies in the Donbas and other zones of conflict around the world are vital to understanding and confronting hybrid warfare. A failure to continue to learn lessons from this conflict will limit the ability to respond when future incidents of hybrid warfare arise. 🇺🇸

Cyber.Army.Mil - @ArmyCyberInst



ARMY CYBER
INSTITUTE
AT WEST POINT